iPhone OS

Manuale per la distribuzione nel settore aziendale

Prima edizione, per la versione 3.0 o successiva

Apple Inc.
© 2009 Apple Inc. Tutti i diritti riservati.

Questo manuale non può essere copiato, interamente o in parte, senza il consenso scritto di Apple.

Il logo Apple è un marchio di Apple Inc. registrato negli Stati Uniti e in altri paesi. L'uso del logo Apple "tastiera" (Opzione-Maiusc-K) per scopi commerciali senza il previo consenso scritto di Apple può rappresentare una violazione del marchio e costituire concorrenza sleale in violazione delle leggi federali e statali.

Ogni sforzo è stato compiuto per garantire che le informazioni di questo manuale siano accurate. Apple non è responsabile degli eventuali errori di stampa o materiali.

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
+001-408-996-1010
www.apple.com

Apple, il logo Apple, Bonjour, iPod, iTunes, Keychain, Leopard, Mac, Macintosh, il logo Mac, Mac OS, QuickTime, Safari e Tiger sono marchi di Apple Inc. registrati negli Stati Uniti e in altri paesi.

iPhone è un marchio di Apple Inc.

iTunes Store è un marchio di servizio di Apple Inc. registrato negli Stati Uniti e in altri paesi. MobileMe è un marchio di servizio di Apple Inc.

Altri nomi di società e prodotti qui citati sono marchi dei rispettivi proprietari. La citazione di prodotti di terze parti è usata solamente per scopi informativi e non è intesa a scopo pubblicitario o di raccomandazione d'uso. Apple non si assume alcuna responsabilità in merito al funzionamento o all'uso di tali prodotti.

Pubblicato contemporaneamente negli Stati Uniti e in Canada.

T019-1483/06-2009

Indice

Prefazione 5 **iPhone nel settore aziendale**
5 Novità per le aziende in iPhone OS 3.0
6 Requisiti di sistema
7 Microsoft Exchange ActiveSync
9 VPN
10 Protezione di network
10 Certificati e identità
11 Account e-mail
11 Server LDAP
11 Server CalDAV
12 Risorse aggiuntive

Capitolo 1 13 **Deployment di iPhone e iPod touch**
14 Attivare i dispositivi
14 Preparare l'accesso ai servizi del network e ai dati aziendali
19 Determinare le politiche dei codici dei dispositivi
20 Configurare i dispositivi
21 Registrazione e configurazione mediante tecnologia over the air
26 Altre risorse

Capitolo 2 27 **Creare e distribuire i profili di configurazione**
27 Informazioni su Utility Configurazione iPhone
29 Creare profili di configurazione
39 Modificare i profili di configurazione
39 Installare profili di fornitura e applicazioni
39 Installare i profili di configurazione
43 Rimuovere e aggiornare i profili di configurazione

Capitolo 3 44 **Configurare manualmente i dispositivi**
44 Impostazioni VPN
48 Impostazioni Wi-Fi
49 Impostazioni di Exchange
54 Installare identità e certificati root
55 Account e-mail aggiuntivi
55 Aggiornare e rimuovere i profili
55 Altre risorse

Capitolo 4 56 **Distribuire iTunes**
56 Installazione di iTunes
58 Attivazione rapida dei dispositivi con iTunes
59 Configurazione delle limitazioni di iTunes
61 Creare un backup di iPhone con iTunes

Capitolo 5 62 **Distribuire le applicazioni per iPhone**
62 Registrarsi per lo sviluppo di applicazioni
63 Firmare le applicazioni
63 Creare il profilo di fornitura per la distribuzione
63 Installare i profili di fornitura mediante iTunes
64 Installare profili di fornitura con Utility Configurazione iPhone
64 Installare applicazioni mediante iTunes
65 Installare applicazioni con Utility Configurazione iPhone
65 Utilizzare le applicazioni aziendali
65 Disabilitare un'applicazione aziendale
65 Altre risorse

Appendice A 66 **Configurazione dei server VPN Cisco**
66 Piattaforme Cisco supportate
66 Metodi di autenticazione
67 Gruppi di autenticazione
67 Certificati
68 Impostazioni di IPSec
68 Altre funzionalità supportate

Appendice B 69 **Formato dei profili di configurazione**
69 Livello base
70 Contenuto del payload
71 Payload password rimozione profilo
71 Payload Politica codice
73 Payload e-mail
74 Payload clip web
74 Payload LDAP
75 Payload CalDAV
75 Payload sottoscrizione calendario
76 Payload SCEP
76 Payload APN
77 Payload Exchange
78 Payload di VPN
80 Payload Wi-Fi
83 Esempi di profili di configurazione

iPhone nel settore aziendale

Impara come integrare iPhone e iPod touch nei sistemi aziendali.

Questa guida è destinata agli amministratori di sistema e fornisce informazioni sulla distribuzione e il supporto di iPhone e iPod touch all'interno degli ambienti aziendali.

Novità per le aziende in iPhone OS 3.0

iPhone OS 3.0 include numerosi miglioramenti, compresi i seguenti potenziamenti ottimizzati per gli utenti aziendali.

- Supporto della sincronizzazione wireless con calendario CalDAV.
- Supporto server LDAP per la ricerca di contatti nei messaggi e-mail, nella rubrica e nei messaggi SMS.
- Possibilità di codicare e bloccare i profili di configurazione su un dispositivo in modo che possano essere rimossi solo inserendo una password amministratore.
- Utilizzo di Utility Configurazione iPhone 2.0 per aggiungere e rimuovere i profili di configurazione codificati direttamente sui dispositivi collegati al computer via USB.
- Supporto del protocollo OCSP (Online Certificate Status Protocol) per la revoca dei certificati.
- Supporto delle connessioni VPN su richiesta, basate su certificato.
- Supporto della configurazione proxy VPN mediante profilo di configurazione e server VPN.
- Possibilità per gli utenti Microsoft Exchange di invitare gli altri utenti alle riunioni. Possibilità per gli utenti Microsoft Exchange 2007 di visualizzare lo stato della risposta.
- Supporto dell'autenticazione mediante certificato di client Exchange ActiveSync.
- Supporto delle politiche EAS aggiuntive, insieme al protocollo 12.1 EAS.
- Disponibilità delle restrizioni al dispositivo, compresa la possibilità di specificare il periodo di tempo durante il quale il dispositivo può rimanere senza blocco e la possibilità di disabilitare la fotocamera.

- Possibilità di effettuare ricerche nei messaggi e-mail locali e negli eventi calendario. Per IMAP, MobileMe e Exchange 2007, possibilità di effettuare ricerche anche nei messaggi e-mail che si trovano sul server.
- Possibilità di indicare cartelle e-mail aggiuntive per la consegna dei messaggi e-mail push.
- Possibilità di specificare le impostazioni proxy APN utilizzando un profilo di configurazione.
- Possibilità di installare i clip web utilizzando un profilo di configurazione.
- Supporto di 02.1x EAP-SIM.
- Possibilità di autenticare e registrare i dispositivi "over the air", utilizzando un server SCEP (Simple Certificate Enrollment Protocol).
- Possibilità di utilizzare iTunes per archiviare i backup del dispositivo in formato codificato.

Requisiti di sistema

Questa sezione contiene una panoramica dei requisiti del sistema e dei vari componenti disponibili per l'integrazione di iPhone e iPod touch con i sistemi aziendali.

iPhone e iPod touch

I dispositivi iPhone e iPod touch che utilizzi con il network aziendale devono essere aggiornati con iPhone OS 3.0 o versione successiva.

iTunes

Per procedere alla configurazione di un dispositivo, è necessario disporre di iTunes 8.2 o versione successiva. Questa versione è necessaria anche per installare gli aggiornamenti software per iPhone o iPod touch, installare applicazioni e per sincronizzare musica, video, note o altri dati con Mac o PC.

Per utilizzare iTunes, è necessario un Mac o un PC che disponga di una porta USB 2.0 e soddisfi i requisiti minimi elencati sul sito web di iTunes. Consulta www.apple.com/it/itunes/download/.

Utility Configurazione iPhone

Utility Configurazione iPhone ti consente di creare, codificare e installare i profili di configurazione, individuare e installare i profili di fornitura e le applicazioni autorizzate, acquisire informazioni sul dispositivo compresi i resoconti della console. Per creare profili di configurazione per dispositivi con iPhone OS 3.0 o versione successiva, devi utilizzare Utility Configurazione iPhone 2.0 o versione successiva.

Utility Configurazione iPhone richiede uno dei seguenti sistemi:

- Mac OS X v10.5 Leopard
- Windows XP Service Pack 3 con .NET Framework 3.5 Service Pack 1

- Windows Vista Service Pack 1 con .NET Framework 3.5 Service Pack 1

Utility Configurazione iPhone funziona a 32 bit sulle versioni di Windows a 64 bit.

Puoi scaricare il programma di installazione di .Net Framework 3.5 Service Pack 1 su http://www.microsoft.com/downloads/details.aspx?familyid=ab99342f-5d1a-413d-8319-81da479ab0d7

L'utility ti consente di creare un messaggio in Outlook con un profilo di configurazione come allegato. Inoltre, puoi assegnare nomi utente e indirizzi e-mail dalla tua rubrica ai dispositivi che hai connesso all'utility. Entrambe le funzionalità richiedono Outlook e non sono compatibili con Outlook Express. Per utilizzare tali funzionalità su computer con Windows XP, potrebbe essere necessario installare 2007 Microsoft Office System Update: Redistributable Primary Interop Assemblies. È necessario se Outlook è stato installato prima di .NET Framework 3.5 Service Pack 1.

Il programma di installazione di Primary Interop Assemblies è disponibile su http://www.microsoft.com/downloads/details.aspx?FamilyID=59daebaa-bed4-4282-a28c-b864d8bfa513

Microsoft Exchange ActiveSync

iPhone e iPod touch supportano le seguenti versioni di Microsoft Exchange:

- Exchange ActiveSync for Exchange Server (EAS) 2003 Service Pack 2
- Exchange ActiveSync per Exchange Server (EAS) 2007

Come supporto alle politiche e alle funzionalità di Exchange 2007, è necessario Service Pack 1.

Politiche di Exchange ActiveSync supportate

Sono supportate le seguenti politiche di Exchange:

- Imponi password su dispositivo
- Lunghezza minima password
- Numero massimo di tentativi di inserimento della password
- Richiedi l'uso di numeri e lettere
- Tempo di inattività in minuti

Sono supportate anche le seguenti politiche di Exchange 2007:

- Consenti o proibisci password semplici
- Scadenza password
- Cronologia password
- Intervallo di aggiornamento della politica
- Numero minimo di caratteri complessi nella password

- Richiedi sincronizzazione manuale quando in roaming
- Consenti fotocamera

Per una descrizione di queste politiche, consulta la documentazione di Exchange ActiveSync.

Importante: l'abilitazione della politica "Richiedi l'uso di numeri e lettere" su Exchange 2003 o "Richiedi password alfanumerica" su Exchange 2007 richiede l'inserimento da parte dell'utente di un codice per iPhone che contenga almeno un carattere complesso.

Ripulitura remota

Se necessario, puoi ripulire i contenuti di un dispositivo iPhone o iPod touch. Questa operazione permette di rimuovere tutti i dati e le informazioni di configurazione presenti sul dispositivo, ripristinando le impostazioni originali di fabbrica.

Importante: con alcuni dispositivi, come modelli precedenti di iPhone e iPod touch, l'inizializzazione dei dati può impiegare circa un'ora per ogni 8 GB di capacità del dispositivo. Prima di inizializzare, collega i dispositivi a una fonte di alimentazione. Se il dispositivo si spegne perché la batteria è scarica, il processo di inizializzazione riprende non appena il dispositivo viene collegato all'alimentatore.

Con Exchange Server 2007, puoi avviare una ripulitura remota mediante la console di gestione di Exchange, Outlook Web Access o lo strumento web per l'amministrazione mobile di Exchange ActiveSync.

Con Exchange Server 2003, puoi avviare una ripulitura remota mediante lo strumento web per l'amministrazione mobile di Exchange ActiveSync.

Gli utenti possono ripulire i propri dispositivi scegliendo "Cancella contenuto e impostazioni" dal menu Ripristina delle impostazioni Generali. I dispositivi possono essere inoltre configurati per iniziare automaticamente a ripulire dopo una serie di tentativi di inserimento del codice errati.

Microsoft Direct Push

Exchange ActiveSync invia e-mail, contatti ed eventi del calendario automaticamente a iPhone se è disponibile una connessione dati cellulare o Wi-Fi. iPod touch non dispone di una connessione cellulare, quindi può ricevere le notifiche push solo quando è acceso e collegato a un network Wi-Fi.

Microsoft Exchange Autodiscovery

Il servizio Autodiscover di Exchange Server 2007 è supportato. Durante la configurazione manuale di iPhone o iPod touch, Autodiscover utilizza il tuo indirizzo e-mail e la tua password per determinare automaticamente le informazioni corrette del server Exchange. Per informazioni sull'abilitazione del servizio Autodiscover, vai su http://technet.microsoft.com/en-us/library/cc539114.aspx.

Elenco indirizzi globale di Microsoft Exchange

iPhone e iPod touch ricevono le informazioni sui contatti dall'elenco indirizzi aziendale del server Exchange. È possibile accedere a questa directory durante la ricerca in Contatti; inoltre, l'accesso avviene automaticamente per il completamento degli indirizzi e-mail mentre vengono digitati.

Funzionalità aggiuntive di Exchange ActiveSync supportate

Oltre alle funzionalità e alle proprietà già descritte, iPhone supporta:

- Creazione di inviti calendario. Con Microsoft Exchange 2007, puoi anche visualizzare lo stato delle risposte agli inviti.
- Impostazione dello stato degli inviti su libero, occupato, provvisiorio o fuori sede per gli eventi calendario.
- Ricerca dei messaggi e-mail sul server. Richiede Microsoft Exchange 2007.
- Autenticazione mediante certificato client Exchange ActiveSync.

Funzionalità di Exchange ActiveSync non supportate

Alcune funzionalità di Exchange non sono supportate; ad esempio:

- Gestione delle cartelle
- Apertura di collegamenti nei messaggi e-mail a documenti archiviati su server Sharepoint
- Sincronizzazione delle attività
- Impostazione di un messaggio di risposta "fuori ufficio" automatico
- Contrassegno di messaggi per il completamento

VPN

iPhone e iPod touch possono funzionare con server VPN che supportano i seguenti protocolli e metodi di autenticazione:

- L2TP/IPSec con autenticazione utente mediante password MS-CHAPV2, RSA SecurID e CryptoCard e autenticazione computer mediante chiave condivisa.
- PPTP con autenticazione utente mediante password MS-CHAPV2, RSA SecurID e CryptoCard.
- Cisco IPSec con autenticazione utente tramite password, RSA SecurID o CryptoCard, e autenticazione computer mediante chiave condivisa e certificati. Per ulteriori consigli sulla configurazione e per un elenco dei server VPN Cisco compatibili, consulta l'appendice A.

Cisco IPSec con autenticazione mediante certificato supporta la tecnologia "VPN su richiesta" per i domini specificati durante la configurazione. Consulta "Impostazioni VPN" a pagina 33 per ulteriori dettagli.

Protezione di network

iPhone e iPod touch supportano i seguenti standard di protezione per network wireless 802.11i definiti da Wi-Fi Alliance:

- WEP
- WPA-Personal
- WPA-Enterprise
- WPA2-Personal
- WPA2-Enterprise

Inoltre, iPhone e iPod touch supportano i seguenti metodi di autenticazione 802.1X per network WPA-Enterprise e WPA2-Enterprise:

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0, PEAP v1
- LEAP

Certificati e identità

iPhone e iPod touch possono utilizzare i certificati X.509 con chiavi RSA. Vengono riconosciute le estensioni .cer, .crt e .der. Le valutazioni di catene certificati vengono eseguite con Safari, Mail, VPN e altre applicazioni.

iPhone e iPod touch possono utilizzare documenti P12 (PKCS #12 standard) che contengono esattamente un'identità. Vengono riconosciute le estensioni .p12 e .pfx. Una volta installata un'identità, l'utente riceve la richiesta di inserire una frase chiave per la sua protezione.

I certificati necessari per stabilire la catena certificati a un certificato root attendibile possono essere installati manualmente o utilizzando i profili di configurazione. Non è necessario aggiungere i certificati root forniti sul dispositivo da Apple. Per visualizzare l'elenco dei certificati root di sistema preinstallati, consulta l'articolo del supporto Apple all'indirizzo http://support.apple.com/kb/HT3580.

È possibile installare i certificati in modalità sicura "over the air" mediante SCEP. Per ulteriori informazioni, consulta "Panoramica del processo di registrazione e configurazione" a pagina 21.

Account e-mail

iPhone e iPod touch supportano le soluzioni standard per posta e-mail IMAP4 e POP3 su un'ampia gamma di piattaforme server, tra cui Windows, UNIX, Linux e Mac OS X. Puoi utilizzare anche il protocollo IMAP per accedere alle e-mail degli account Exchange oltre all'account Exchange che utilizzi con la tecnologia push.

Quando un utente effettua una ricerca nei propri messaggi e-mail, può continuare la ricerca sul server di posta. Tale opzione funziona con Microsoft Exchange Server 2007 e con la maggior parte degli account IMAP.

Le informazioni relative all'account e-mail dell'utente, compresi ID utente e password di Exchange, vengono archiviate in modo sicuro sul dispositivo.

Server LDAP

iPhone e iPod touch recuperano le informazioni di contatto delle directory aziendali del server LDAPv3 della tua azienda. Puoi accedere alle directory quando cerchi in Contatti; inoltre, l'accesso è automatico per il completamento degli indirizzi e-mail durante la digitazione.

Server CalDAV

iPhone e iPod touch sincronizzano i dati del calendario con il server CalDAV aziendale. Le modifiche al calendario vengono aggiornate periodicamente tra il dispositivo e il server.

Puoi anche sottoscrivere calendari di sola lettura, come calendari di vacanze o di programmazione di un collega.

Gli account CalDAV non supportano la creazione e l'invio di nuovi inviti calendario da un dispositivo.

Risorse aggiuntive

Oltre a quelle contenute in questa guida, puoi trovare ulteriori informazioni utili nelle pubblicazioni e nei siti web seguenti:

- *Manuale Utente di iPhone*, disponibile per il download all'indirizzo www.apple.com/it/support/iphone/.Per visualizzare il manuale di iPhone, tocca il preferito "Manuale Utente di iPhone" in Safari o vai su http://help.apple.com/it/iphone/.
- Tour guidato di iPhone su www.apple.com/it/iphone/guidedtour/
- Tour guidato di iPod touch su www.apple.com/it/ipodtouch/guidedtour/
- Pagina web di iPhone, all'indirizzo www.apple.com/it/iphone/
- Pagina web di iPod touch, all'indirizzo www.apple.com/it/ipodtouch/
- Manuale Utente di iPod touch, disponibile per il download all'indirizzo www.apple.com/it/support/ipodtouch/.Per visualizzare il manuale di iPod touch, tocca il preferito "Manuale Utente di iPod touch" in Safari o vai su http://help.apple.com/it/ipodtouch/.
- Pagina web di iPhone nel settore aziendale, all'indirizzo www.apple.com/it/iphone/enterprise/
- Pagina web di supporto per iPhone, all'indirizzo www.apple.com/it/support/iphone/
- Pagina web di supporto per iPod touch, all'indirizzo www.apple.com/it/support/ipodtouch/
- Pagina web di iTunes all'indirizzo www.apple.com/it/itunes/
- Panoramica dei prodotti per Microsoft Exchange all'indirizzo http://technet.microsoft.com/en-us/library/bb124558.aspx
- Deployment di Exchange ActiveSync, all'indirizzo http://technet.microsoft.com/en-us/library/aa995962.aspx
- Libreria di documentazione tecnica di Microsoft Exchange 2003 all'indirizzo http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx
- Gestione della sicurezza di Exchange ActiveSync, all'indirizzo http://technet.microsoft.com/en-us/library/bb232020(EXCHG.80).aspx
- Pagina web Wi-Fi for Enterprise all'indirizzo www.wi-fi.org/enterprise.php
- Connettività VPN di iPhone ai dispositivi di sicurezza adattativi Cisco (ASA) su www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/iPhone/2.0/connectivity/guide/iphone.html

Deployment di iPhone e iPod touch

1

Questo capitolo contiene una panoramica su come effettuare il deployment di iPhone e iPod touch all'interno di un'azienda.

iPhone e iPod touch sono progettati per integrarsi facilmente con sistemi aziendali quali Microsoft Exchange 2003 e 2007, network wireless sicuri basati sui protocolli 802.1X e network privati virtuali Cisco IPSec. Come avviene per qualsiasi soluzione aziendale, una buona pianificazione e la comprensione delle opzioni disponibili per la distribuzione rendono questa operazione più facile ed efficiente per amministratori e utenti.

Durante la pianificazione della distribuzione di iPhone e iPod touch, è necessario considerare quanto segue:

- In che modo sarà attivato l'uso di servizi cellulari wireless sui dispositivi iPhone aziendali?
- A quali servizi di network, applicazioni e dati aziendali dovranno accedere gli utenti?
- Quali politiche desideri impostare sui dispositivi al fine di proteggere i dati aziendali riservati?
- Desideri configurare manualmente i singoli dispositivi o utilizzare un processo semplificato per la configurazione di un grande numero di apparecchi?

Le specifiche relative ad ambiente aziendale, politiche IT e operatore wireless e i requisiti di elaborazione e comunicazione hanno effetto sul modo in cui è possibile personalizzare la strategia di distribuzione.

Attivare i dispositivi

Prima di poter essere utilizzato per effettuare e ricevere chiamate, inviare messaggi di testo o connettersi a un network dati cellulare, ogni iPhone deve essere attivato dal proprio gestore wireless. Contatta l'operatore per informazioni sulle tariffe per voce e dati e istruzioni di attivazione per i clienti del settore consumer e aziendali.

Tu o l'utente dovete installare una scheda SIM all'interno di iPhone. Quindi, per completare il processo di attivazione, iPhone deve essere connesso a un computer dotato di iTunes. Se la scheda SIM è già attiva, iPhone è pronto per essere usato; in caso contrario, iTunes ti guida attraverso il processo di attivazione di una nuova linea di servizio.

Anche se attualmente non è disponibile alcun servizio cellulare o scheda SIM per iPod touch, per poterlo sbloccare questo deve essere collegato a un computer su cui è installato iTunes.

Dal momento che iTunes è necessario per completare il processo di attivazione di iPhone e iPod touch, devi decidere se desideri installare iTunes sul computer Mac o sul computer PC di ciascun utente o se preferisci completare personalmente l'operazione per ogni dispositivo utilizzando iTunes sul tuo computer.

Dopo l'attivazione, non è necessario usare iTunes per utilizzare il dispositivo con i sistemi aziendali, ma è necessario utilizzarlo per eseguire la sincronizzazione di musica, video e preferiti del browser web con il computer. Inoltre, iTunes è necessario anche per scaricare e installare gli aggiornamenti software per i dispositivi e installare le applicazioni aziendali.

Per ulteriori informazioni sull'attivazione di dispositivi e sull'utilizzo di iTunes, consulta il capitolo 4

Preparare l'accesso ai servizi del network e ai dati aziendali

Il software iPhone OS 3.0 consente l'invio sicuro di messaggi e-mail, contatti e calendari push verso le soluzioni Microsoft Exchange Server 2003 o 2007 esistenti, oltre a rafforzare le politiche relative a GAL (Global Address Lookup), Remote Wipe (cancellazione remota) e codice del dispositivo. Il software permette anche agli utenti di connettersi in modo sicuro alle risorse aziendali tramite network wireless WPA Enterprise e WPA2 Enterprise che utilizzano l'autenticazione wireless 802.1X e/o tramite VPN che utilizzano i protocolli PPTP, LT2P su IPSec o Cisco IPSec.

Se la società non utilizza Microsoft Exchange, gli utenti possono usare comunque i propri iPhone o iPod touch per sincronizzare le informazioni in modalità wireless con la maggior parte dei server e dei servizi basati sugli standard POP o IMAP. Inoltre, essi possono utilizzare iTunes per sincronizzare gli eventi del calendario e i contatti con iCal e Address Book per Mac OS X o con Microsoft Outlook su un PC. Per l'accesso wireless a calendari e directory, sono supportati CalDAV e LDAP.

Per determinare a quali servizi del network devono poter accedere gli utenti, occorre tenere in considerazione quanto segue:

Microsoft Exchange

iPhone comunica direttamente con il server Microsoft Exchange tramite il protocollo Microsoft EAS (Exchange ActiveSync). Exchange ActiveSync gestisce una connessione tra il server Exchange e iPhone in modo da aggiornare immediatamente iPhone quando viene ricevuto un nuovo messaggio e-mail o un invito a una riunione. iPod touch non dispone di una connessione cellulare, pertanto può ricevere le notifiche push solo quando è acceso e collegato a un network Wi-Fi.

Se la società supporta Exchange ActiveSync su Exchange Server 2003 o Exchange Server 2007, i servizi necessari sono già disponibili. Per Exchange Server 2007, assicurati che sia installato Client Access Role (Ruolo Accesso client). Per Exchange Server 2003, assicurati di aver abilitato Outlook Mobile Access (OMA).

Se disponi di un server Exchange ma la società ha appena iniziato a usare Exchange ActiveSync, puoi consultare i seguenti argomenti:

Configurazione di un network

- Verifica che la porta 443 del firewall sia aperta. Se la società utilizza Outlook Web Access, molto probabilmente la porta 443 è già aperta.
- Controlla che il certificato di un server sia installato sul server frontale di Exchange e attiva solo l'autenticazione di base, nelle proprietà del metodo di autenticazione, per richiedere una connessione SSL alla directory Microsoft Server ActiveSync dei tuoi IIS.
- Quando utilizzi un server Microsoft ISA (Internet Security and Acceleration), verifica che sia installato un certificato server e aggiorna il DNS pubblico affinché sia in grado di risolvere correttamente le connessioni in entrata.
- Assicurati che il DNS del network restituisca al server Exchange ActiveSync un singolo indirizzo indirizzabile dall'esterno per i client intranet e Internet. Questo requisito è necessario per fare in modo che il dispositivo possa utilizzare lo stesso indirizzo IP per comunicare con il server quando sono attivi entrambi i tipi di connessione.
- Se utilizzi un server ISA, crea un web listener e una regola di pubblicazione accesso per i client web Exchange. Per ulteriori informazioni, consulta la documentazione Microsoft.
- Per tutti i firewall e i dispositivi del network, imposta su 30 minuti il timeout di sessione inattiva. Per informazioni su heartbeat e intervalli di timeout, consulta la documentazione di Microsoft Exchange su http://technet.microsoft.com/en-us/library/cc182270.aspx.

Configurazione degli account Exchange

- Abilita Exchange ActiveSync per utenti o gruppi specifici che utilizzano il servizio Active Directory. In Exchange Server 2003 ed Exchange Server 2007, vengono abilitati di default su tutti i dispositivi portatili a livello organizzativo. Per Exchange Server 2007, consulta la documentazione relativa alla configurazione dei destinatari nella Console Gestione di Exchange.
- Configura le funzionalità mobili, le politiche e le impostazioni di protezione dei dispositivi mediante il Gestore di sistema di Exchange. Per Exchange Server 2007, ciò è possibile tramite la Console Gestione di Exchange.
- Scarica e installa lo strumento Microsoft Exchange ActiveSync Mobile Administration Web Tool, necessario per eseguire operazioni di pulitura remota. In Exchange Server 2007, la pulitura remota può essere avviata anche mediante Outlook Web Access o tramite la Console Gestione di Exchange.

Network Wi-Fi WPA/WPA2 Enterprise

Il supporto di WPA Enterprise e WPA2 Enterprise garantisce che i network wireless aziendali siano accessibili in modo sicuro da iPhone e iPod touch. WPA/WPA2 Enterprise utilizza la crittografia AES a 128 bit, un collaudato metodo di codificazione basato sull'uso di blocchi e che fornisce un elevato livello di protezione per i dati aziendali.

Grazie al supporto dell'autenticazione 802.1X, iPhone e iPod touch possono essere integrati in un'ampia gamma di ambienti server RADIUS. Sono supportati i metodi di autenticazione wireless 802.1X, tra cui EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 e LEAP.

Configurare un network WPA/WPA2 Enterprise

- Verifica la compatibilità dei dispositivi del network e seleziona un tipo di autenticazione (tipo EAP) supportato da iPhone e iPod touch. Assicurati che 802.1X sia attivato sul server di autenticazione e se necessario installa un certificato server, quindi assegna a utenti e gruppi le autorizzazioni di accesso al network.
- Configura i punti di accesso wireless per l'autenticazione 802.1X e inserisci le informazioni relative ai corrispondenti server RADIUS.
- Verifica la distribuzione 802.1X con un Mac o un PC per assicurarti che l'autenticazione RADIUS sia configurata correttamente.
- Se prevedi di utilizzare l'autenticazione basata su certificati, verifica che l'infrastruttura di chiavi pubbliche sia configurata in modo da supportare dispositivi e certificati utente con il relativo processo di distribuzione delle chiavi.
- Controlla la compatibilità del formato dei certificati con il dispositivo e con il server di autenticazione. Per informazioni sui certificati, consulta "Certificati e identità" a pagina 10.

Network privati virtuali

L'accesso protetto ai network privati è supportato su iPhone e iPod touch tramite i protocolli per i network privati virtuali Cisco IPSec, L2TP su IPSec e PPTP. Se l'organizzazione supporta uno di questi protocolli, per utilizzare i dispositivi con l'infrastruttura della VPN non è necessario eseguire alcuna ulteriore configurazione o installazione di applicazioni di terze parti.

Le distribuzioni Cisco IPSec possono sfruttare i vantaggi offerti dall'autenticazione basata su certificati tramite i certificati digitali standard x.509. Inoltre, l'autenticazione mediante certificato ti consente di sfruttare "VPN su richiesta", che fornisce accesso wireless sicuro e continuo al network aziendale.

Per l'autenticazione basata su due token, iPhone e iPod touch supportano RSA SecurID e CryptoCard. Durante la creazione di una connessione a una VPN, gli utenti possono inserire i propri PIN e le proprie password monouso generate mediante token direttamente sul dispositivo. Per ulteriori consigli sulla configurazione e per un elenco dei server VPN Cisco compatibili, consulta l'appendice A.

iPhone e iPod touch supportano anche l'autenticazione mediante una chiave condivisa per distribuzioni Cisco IPSec e L2TP su IPSec, oltre a MS-CHAPv2 per l'autenticazione base tramite nome utente e password.

È supportata anche la configurazione automatica di "Proxy VPN" (PAC e WPAD), che ti consente di specificare le impostazioni del server proxy per accedere a URL specifici.

Linee guida per la configurazione di una VPN

- iPhone è in grado di integrarsi con la maggior parte dei network VPN con il minimo impegno di configurazione per abilitarne l'accesso al proprio network. Il modo migliore per prepararsi alla distribuzione consiste nel verificare che i protocolli VPN aziendali e i metodi di autenticazione esistenti siano supportati da iPhone.
- Verifica la compatibilità con gli standard dai concentratori della VPN. Spesso è utile anche rivedere il percorso di autenticazione verso il server RADIUS o di autenticazione per assicurarsi che gli standard supportati da iPhone siano abilitati nella propria implementazione.
- Contatta i fornitori di soluzioni per accertarti che le attrezzature e il software impiegati dispongano dei più recenti aggiornamenti di protezione e di firmware.
- Se desideri configurare delle impostazioni proxy per un URL specifico, posiziona un documento PAC su un server web accessibile con impostazioni VPN di base e assicurati che sia servito da un tipo MIME application/x-ns-proxy-autoconfig. In alternativa, configura il DNS o DHCP per fornire la posizione di un documento WPAD su un server accessibile in modo simile.

E-mail IMAP

Se la società non utilizza Microsoft Exchange, è comunque possibile implementare una soluzione e-mail sicura e basata su standard utilizzando un server di posta elettronica in grado di supportare il protocollo IMAP e configurato in modo da richiedere l'autenticazione dell'utente e l'uso del protocollo SSL. Questi server possono essere ubicati all'interno di un subnetwork DMZ, dietro un firewall aziendale o in una loro combinazione.

Tramite SSL, iPhone e iPod touch supportano la crittografia a 128 bit e i certificati X.509 emessi dalle principali autorità di certificazione. Essi supportano anche i metodi di autenticazione dettagliata tra cui lo standard MD5 Challenge-Response e NTLMv2.

Linee guida per la configurazione di network IMAP

- Per garantire una maggiore protezione, installa sul server un certificato digitale rilasciato da una CA (autorità di certificazione) considerata attendibile. L'installazione di un certificato emesso da una CA è un passo importante per garantire che il server proxy sia un'entità considerata attendibile nell'ambito dell'infrastruttura aziendale. Consulta "Impostazioni delle credenziali" a pagina 37 per informazioni sull'installazione dei certificati su iPhone.
- Per consentire ai dispositivi iPhone e iPod touch di ricevere messaggi e-mail dal server, apri la porta 993 nel firewall e assicurati che il server proxy sia impostato in modo da utilizzare IMAP su SSL.
- Per consentire ai dispositivi di inviare messaggi e-mail, devono essere aperte le porte 587, 465 o 25. La porta 587 viene usata per prima e rappresenta la scelta migliore.

Directory LDAP

iPhone OS 3.0 o versione successiva ti consente di accedere ai server directory basati sullo standard LDAP. Questo ti consente di aggiungere una directory a indirizzo globale o altre informazioni simili all'elenco GAL (Elenco indirizzi globale) di Microsoft Exchange.

Quando sul dispositivo viene configurato un account LDAP, il dispositivo cerca l'attributo `namingContexts` al livello root del server per identificare la base di ricerca di default. Di default, l'ambito di ricerca è impostato al livello del sottoalbero.

Calendari CalDAV

Il supporto CalDAV in iPhone OS 3.0 o versione successiva può essere utilizzato per fornire calendari globali e programmazioni per organizzazioni che non utilizzano Microsoft Exchange. iPhone funziona con server calendario che supportano lo standard CalDAV.

Calendari sottoscritti

Se desideri pubblicare dei calendari di sola lettura di eventi aziendali, come vacanze o programmazioni di eventi speciali, iPhone può sottoscrivere dei calendari e visualizzare le informazioni accanto ai calendari Microsoft Exchange e CalDAV. iPhone funziona con documenti calendario nel formato standard iCalendar (.ics).

Applicazioni aziendali

Se prevedi di distribuire applicazioni aziendali per iPhone e iPod touch, puoi installarle sui dispositivi mediante "Utility Configurazione iPhone" o iTunes. Una volta distribuita un'applicazione sui dispositivi degli utenti, l'aggiornamento di tale applicazione sarà più semplice se ogni utente dispone di iTunes installato sul proprio Mac o PC.

Determinare le politiche dei codici dei dispositivi

Dopo aver deciso a quali servizi del network e dati gli utenti dovranno poter accedere, devi stabilire le politiche da implementare per i codici dei dispositivi.

L'obbligo di impostare dei codici sul proprio dispositivo è consigliato per le aziende in cui l'accesso a network, sistemi o applicazioni non richiede alcuna password o token di autenticazione. Se utilizzi l'autenticazione basata su certificati per un network 802.1X o una VPN Cisco IPSec, oppure se l'applicazione aziendale registra le credenziali di accesso, è necessario richiedere agli utenti di impostare un codice del dispositivo con un periodo di timeout breve, in modo da evitare che un dispositivo smarrito o sottratto indebitamente possa essere impiegato senza il relativo codice.

Le politiche possono essere impostate su iPhone e iPod touch in uno dei due modi descritti di seguito. Se il dispositivo è configurato in modo da accedere a un account Microsoft Exchange, le politiche di Exchange ActiveSync vengono inviate al dispositivo tramite un collegamento wireless. Ciò permette di imporre e aggiornare le politiche senza alcuna azione da parte dell'utente. Per informazioni sulle politiche EAS, consulta "Politiche di Exchange ActiveSync supportate" a pagina 7.

Se la società non utilizza Microsoft Exchange, puoi impostare politiche simili sui dispositivi mediante la creazione di profili di configurazione. Quando modifichi una politica, devi pubblicare o inviare il profilo aggiornato agli utenti oppure installare il profilo con "Utility Configurazione iPhone". Per informazioni sulle politiche di codice del dispositivo, consulta "Impostazioni dei codici" a pagina 31.

Configurare i dispositivi

A questo punto devi decidere come procedere per configurare i dispositivi iPhone e iPod touch. Questa operazione dipende principalmente dal numero di dispositivi che si prevede di distribuire e gestire nel tempo. Se questo numero è relativamente ridotto, può risultare più semplice per lamministratore e gli utenti configurare manualmente i singoli dispositivi. Questa operazione richiede l'utilizzo del dispositivo per inserire le impostazioni di ogni account e-mail e del Wi-Fi nonché le informazioni di configurazione della VPN. Per ulteriori informazioni sulla configurazione manuale, consulta il capitolo 3.

Se prevedi di distribuire un'ampia serie di dispositivi o devi gestire un numero elevato di impostazioni di e-mail e network e di certificati da installare, può essere utile configurare i dispositivi mediante la creazione e la distribuzione di profili di configurazione. I profili di configurazione consentono di caricare rapidamente sul dispositivo le informazioni relative a impostazioni e autorizzazioni. Inoltre, alcune impostazioni di VPN e Wi-Fi possono essere specificate solamente mediante un profilo di configurazione; se non utilizzi Microsoft Exchange, dovrai usare un profilo di configurazione anche per impostare le politiche di codice del dispositivo.

I profili di configurazione possono essere codificati e firmati; questo ti consente di restringerne l'uso a un dispositivo specifico e impedisce che le impostazioni contenute nel profilo possano essere modificate da chiunque. Inoltre, puoi contrassegnare un profilo come bloccato, affinché dopo averlo installato non possa essere rimosso senza inizializzare tutti i dati presenti sul dispositivo oppure, facoltativamente, senza un codice amministratore.

Indipendentemente dall'uso o meno della configurazione manuale dei dispositivi o mediante i profili di configurazione, devi decidere anche se configurare i dispositivi o delegare questa operazione agli utenti. Il comportamento prescelto dipende dall'ubicazione degli utenti, dalle politiche aziendali in merito alla possibilità degli utenti di gestire le proprie attrezzature IT e dalla complessità della configurazione del dispositivo che intendi distribuire. I profili di configurazione sono più adatti alle grandi aziende, ai dipendenti che lavorano in sedi remote o per gli utenti che non sono in grado di eseguire personalmente tali operazioni sui propri dispositivi.

Se desideri consentire agli utenti di attivare personalmente i propri dispositivi e installare o aggiornare le applicazioni aziendali, iTunes deve essere installato sui loro Mac o PC. iTunes è necessario anche per gli aggiornamenti del software di iPhone e iPod touch, pertanto è utile ricordarlo se decidi di non distribuire iTunes agli utenti. Per informazioni su come distribuire iTunes, consulta il capitolo 4.

Registrazione e configurazione mediante tecnologia over the air

Registrazione si riferisce al procedimento di autenticazione di un dispositivo e di un utente affinché sia possibile automatizzare il processo di distribuzione dei certificati. I certificati digitali offrono molti benefici agli utenti iPhone. Possono essere utilizzati per autenticare l'accesso ai servizi aziendali, come i network wireless Microsoft Exchange ActiveSync, WPA2 Enterprise e le connessioni aziendali VPN. L'autenticazione sulla base del certificato ti consente anche di utilizzare la tecnologia "VPN su richiesta" per l'accesso wireless a network aziendali.

Oltre ad utilizzare le funzionalità di registrazione "over the air" per rilasciare certificati per l'infrastruttura a chiave pubblica (PKI: Public Key Infrastructure) della tua azienda, puoi anche effettuare il deployment dei profili di configurazione del dispositivo. In questo modo l'accesso ai servizi aziendali sarà consentito solo agli utenti considerati attendibili e i cui dispositivi siano configurati secondo le politiche IT. Poiché i profili di configurazione possono essere sia codificati che bloccati, le impostazioni non possono essere rimosse, modificate o condivise con altri. Queste funzionalità sono disponibili mediante procedimento "over the air", come descritto di seguito, e anche con "Utility Configurazione iPhone" per configurare i dispositivi mentre sono collegati al computer amministratore. Per informazioni sull'uso di "Utility Configurazione iPhone", consulta il capitolo 2.

L'implementazione della registrazione e della configurazione "over the air" richiede lo sviluppo e l'integrazione dei servizi di autenticazione, directory e certificazione. È possibile effettuarne il deployment utilizzando servizi web standard; dopo aver effettuato la registrazione, gli utenti potranno configurare i propri dispositivi in modo sicuro e autenticato.

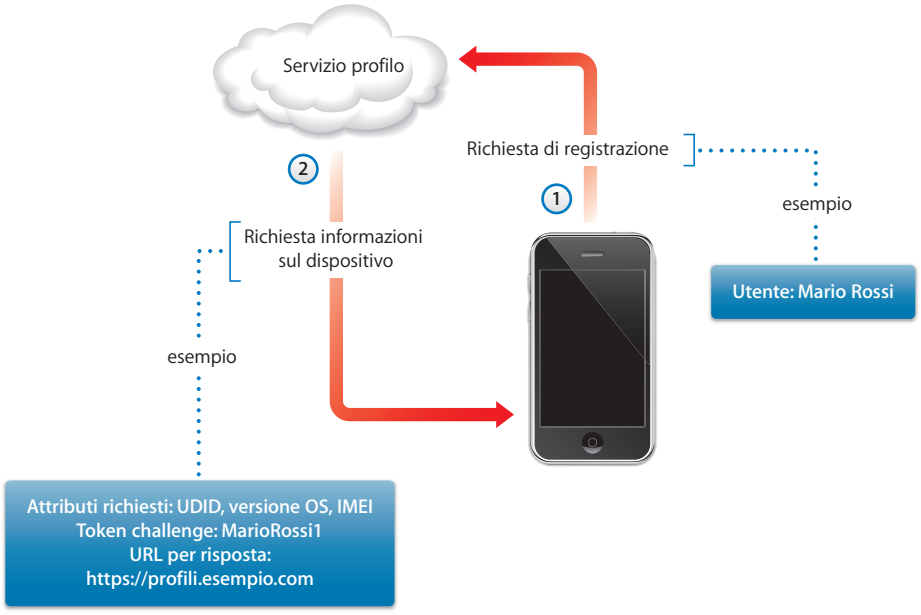
Panoramica del processo di registrazione e configurazione

Per implementare questo processo devi creare il tuo *servizio profili* che accetti connessioni HTTP, autentichi gli utente, crei profili mobileconfig e gestisca il processo generale descritto in questa sezione.

Per rilasciare le credenziali del dispositivo utilizzando il protocollo SCEP (Simple Certificate Enrollment Protocol), è necessaria un'autorità di certificazione (CA). Sia Cisco IOS che Microsoft Server 2003, con l'estensione per i servizi di certificazione, supportano il protocollo SCEP. Consulta "Altre risorse" a pagina 26 per collegamenti a PKI, SCEP e argomenti correlati.

La seguente sezione descrve il processo di registrazione e configurazione supportato da iPhone.

Fase 1: inizio della registrazione

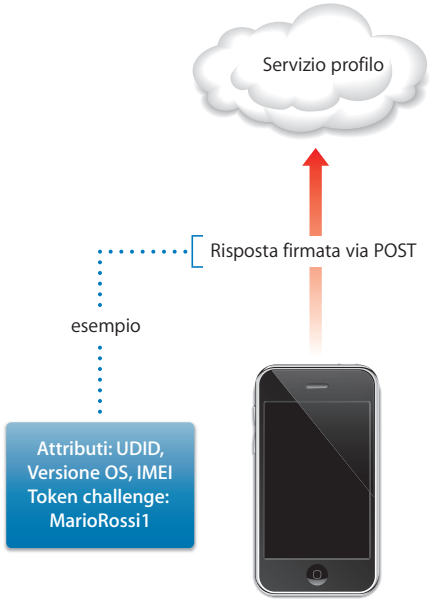


Fase 1: inizio della registrazione. La registrazione inizia quando l'utente, mediante Safari, accede all'URL del servizio profili che hai creato. Questa azione rappresenta la richiesta di registrazione (il passo 1 del diagramma) e dovresti autenticare l'identità dell'utente. Puoi optare per un'autenticazione di base oppure associare l'identità dell'utente a servizi directory già esistenti.

Al passo 2, il tuo servizio invia un profilo di configurazione (.mobileconfig) in risposta. In tale risposta è specificato un'elenco di attributi che il dispositivo deve fornire nella prossima risposta oltre a una chiave pre-condivisa (challenge) che può portare avanti l'identità dell'utente durante il processo, in modo che sia possibile personalizzare il processo di configurazione per ogni utente. Gli attributi del dispositivo che il servizio può richiedere sono: versione iPhone OS, ID del dispositivo (indirizzo MAC), tipo di prodotto (iPhone o iPod touch), ID del telefono (IMEI) e informazioni relative alla SIM (ICCID).

Per un esempio del profilo di configurazione di questa fase, consulta "Esempio fase 1 risposta del server" a pagina 83.

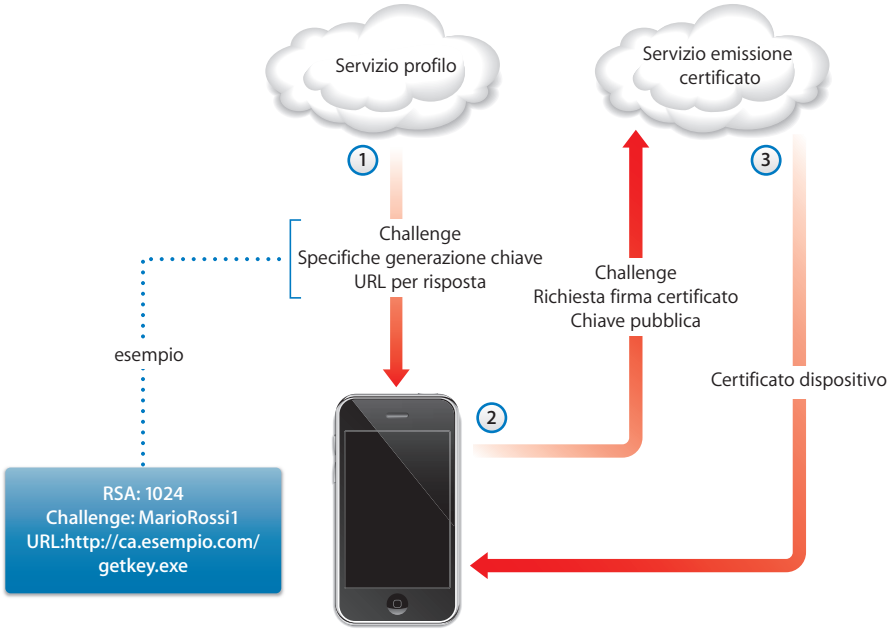
Fase 2: autenticazione del dispositivo



Fase 2: autenticazione del dispositivo. Dopo l'accettazione da parte dell'utente dell'installazione del profilo ricevuto nella fase 1, il dispositivo cerca gli attributi richiesti, aggiunge la risposta di verifica (se fornita) e firma la risposta utilizzando l'dentità integrata del dispositivo (certificato rilasciato da Apple) e lo invia nuovamente al server mediante HTTP Post.

Per un profilo di configurazione campione di questa fase, consulta "Esempio fase 2 risposta del dispositivo" a pagina 84.

Fase 3: installazione del certificato



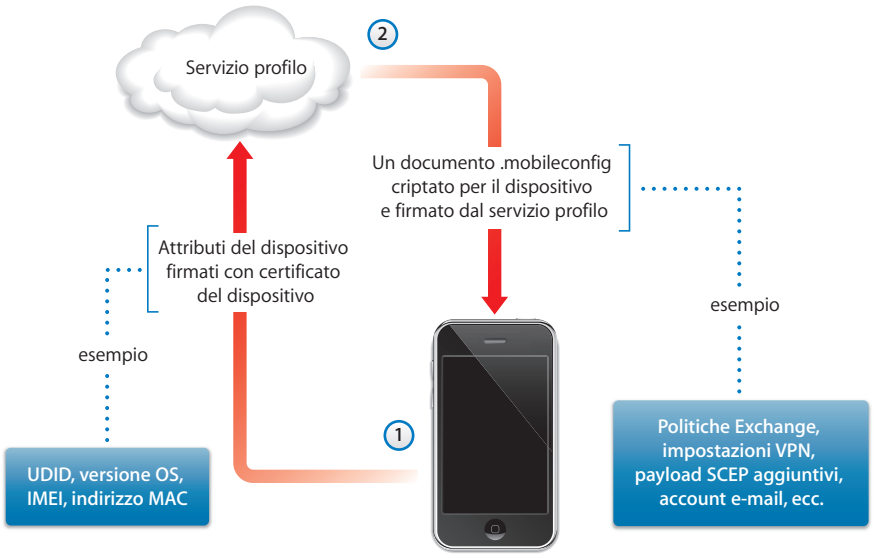
Fase 3: installazione del certificato. Al passo 1, il servizio profili risponde con specificazioni utilizzate dal dispositivo per generare una chiave (RSA 1024) e restituirla per la certificazione mediante protocollo SCEP (Simple Certificate Enrollment Protocol).

Al passo 2, la richiesta SCEP deve essere gestita in modalità automatica, utilizzando la verifica del pacchetto SCEP per autenticare la richiesta.

Al passo 3, la CA risponde con un certificato di codificazione per il dispositivo.

Per un profilo di configurazione campione di questa fase, consulta "Esempio fase 3 risposta del server con specifiche SCEP" a pagina 85.

Fase 4: configurazione del dispositivo



Fase 4: configurazione del dispositivo. Al passo 1, il dispositivo risponde con un elenco di attributi, firmati con il certificato di codificazione fornito dalla CA durante la fase precedente.

Al passo 2, il servizio profili risponde con un documento .mobileconfig codificato che viene installato automaticamente. Il server del profilo dovrebbe firmare il documento .mobileconfig. Il certificato SSL può essere utilizzato a tale scopo, per esempio.

Oltre alle impostazioni generali, questo profilo di configurazione dovrebbe anche definire le politiche aziendali che desideri far osservare; dovrebbe trattarsi di un profilo protetto, in modo che l'utente non possa rimuoverlo dal dispositivo. Il profilo di configurazione può contenere richieste aggiuntive di registrazione di identità mediante protocollo SCEP, che verranno eseguite dopo l'installazione del profilo.

Per un profilo di configurazione campione di questa fase, consulta "Esempio fase 4 risposta del dispositivo" a pagina 86.

Altre risorse

- PKI dei certificati digitali per IPSec VPN su https://cisco.hosted.jivesoftware.com/docs/DOC-3592
- PKI (Public Key Infrastructure) su http://en.wikipedia.org/wiki/Public_key_infrastructure
- Guida al funzionamento di PKI di Windows Server 2003 su http://www.microsoft.com/downloads/details.aspx?familyid=8E25369F-BC5A-4083-A42D-436BDB363E7E&displaylang=en
- Specifica del protocollo SCEP IETF su http://www.ietf.org/internet-drafts/draft-nourse-scep-18.txt

Informazioni e risorse aggiuntive sull'utilizzo di iPhone e iPod touch nel settore aziendale sono disponibili all'indirizzo http://www.apple.com/it/iphone/enterprise/.

Creare e distribuire i profili di configurazione

2

I profili di configurazione definiscono il modo in cui iPhone e iPod touch operano nell'ambito dei sistemi aziendali.

I profili di configurazione sono documenti XML che contengono politiche di sicurezza e restrizioni sui dispositivi, informazioni sulla configurazione VPN, impostazioni Wi-Fi, account e-mail e calendario e credenziali di autenticazione che consentono a iPhone e iPod touch di funzionare con i sistemi aziendali.

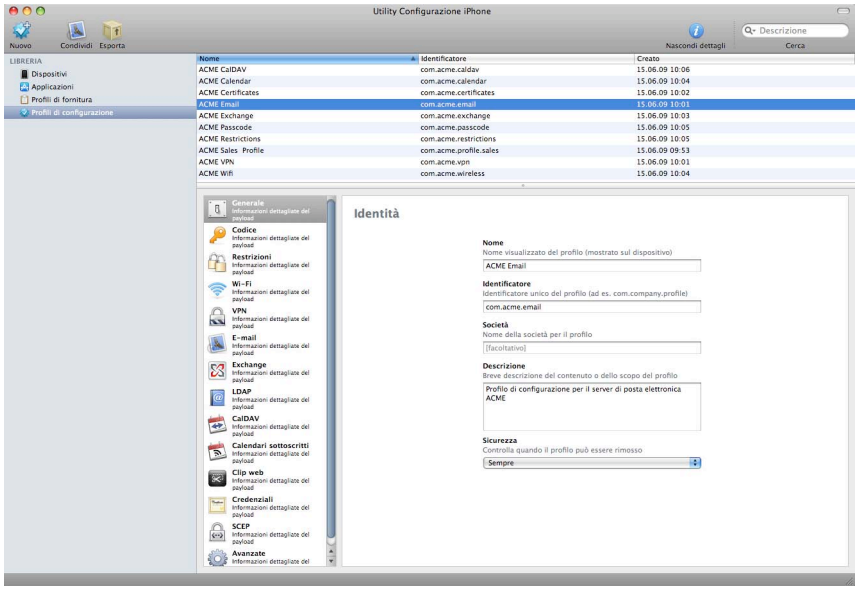
Puoi installare i profili di configurazione sui dispositivi collegati al computer tramite USB, utilizzando "Utility Configurazione iPhone" oppure puoi distribuire i profili di configurazione via e-mail o utilizzando una pagina web. Quando gli utenti aprono l'allegato di un messaggio e-mail o scaricano il profilo sul proprio dispositivo utilizzando Safari, il sistema chiede loro di avviare il processo di installazione.

Se preferisci non creare e distribuire i profili di configurazione, puoi configurare manualmente i dispositivi iPhone o iPod touch. Per informazioni sulle configurazioni manuali, consulta il capitolo 3.

Informazioni su Utility Configurazione iPhone

Puoi utilizzare "Utility Configurazione iPhone" per creare, codificare e installare i profili di configurazione in modo semplice e veloce, per individuare e installare profili di fornitura e applicazioni autorizzate e per acquisire informazioni sul dispositivo compresi i resoconti della console. Quando esegui il programma di installazione di Utility Configurazione iPhone, l'applicazione viene installata nella cartella /Applicazioni/Utility/ su Mac OS X oppure nella cartella Programmi\iPhone Configuration Utility\ su Windows.

Quando avvii Utility Configurazione iPhone, viene visualizzata una schermata simile a quella mostrata di seguito.



Il contenuto della sezione principale della finestra varia a seconda delle voci selezionate nella barra laterale.

La barra laterale visualizza la libreria, la quale contiene le seguenti categorie:

- *Dispositivi* mostra l'elenco dei dispositivi iPhone e iPod touch che sono stati connessi al tuo computer.
- *Applicazioni* elenca le applicazioni disponibili per l'installazione sui dispositivi collegati al tuo computer. Per il corretto funzionamento di un'applicazione su un dispositivo, potrebbe essere necessario un profilo di fornitura.
- *Profili di fornitura* elenca i profili che consentono di utilizzare il dispositivo per lo sviluppo dell'OS iPhone, come autorizzato da Apple Developer Connection. Per ulteriori informazioni, consulta il capitolo 5. Inoltre, i profili di fornitura consentono ai dispositivi di eseguire applicazioni aziendali che non vengono distribuite utilizzando iTunes Store.
- *Profili di configurazione* elenca i profili di configurazione creati in precedenza e ti consente di modificare le informazioni immesse o di creare una nuova configurazione che puoi inviare a un utente o installare su un dispositivo collegato.

La barra laterale mostra anche i *Dispositivi collegati*, con informazioni sui dispositivi iPhone o iPod touch attualmente connessi al tuo computer tramite una porta USB. Le informazioni sui dispositivi collegati vengono aggiunte automaticamente all'elenco Dispositivi, in modo che sia possibile vederle nuovamente senza dover ricollegare il dispositivo. Dopo aver collegato un dispositivo, puoi criptare i profili in modo che possano essere utilizzati solo su tale dispositivo.

Quando un dispositivo è collegato, puoi utilizzare "Utility Configurazione iPhone" per installare i profili di configurazione e le applicazioni sul dispositivo. Per dettagli, consulta "Installare profili di configurazione con Utility Configurazione iPhone" a pagina 39,"Installare applicazioni con Utility Configurazione iPhone" a pagina 65 e "Installare profili di fornitura con Utility Configurazione iPhone" a pagina 64.

Quando un dispositivo è collegato, puoi vedere anche i resoconti di console e tutti gli eventuali resoconti di blocco. Questi sono gli stessi resoconti di dispositivo disponibili all'interno dell'ambiente di sviluppo Xcode su Mac OS X.

Creare profili di configurazione

In questo documento ricorrono spesso i termini *profilo di configurazione* e *payload*. Si definisce "profilo di configurazione" l'intero documento usato per configurare alcune impostazioni (singole o multiple) su iPhone o iPod touch. Si definisce "payload" una collezione individuale di un certo tipo di impostazioni, quali le impostazioni VPN, nel profilo di configurazione.

Sebbene sia possibile creare un profilo di configurazione che contenga tutti i payload necessari per l'azienda, considera l'ipotesi di creare un profilo per i certificati e un altro profilo (o più di uno) per altre impostazioni, in modo da poter aggiornare e distribuire ogni tipo di informazione separatamente. Ciò consente anche agli utenti di conservare i certificati già installati in caso di installazione di un nuovo profilo contenente impostazioni per VPN o account.

Molti payload consentono di specificare nomi utente e password. Se ometti questo tipo di informazione, il profilo potrà essere utilizzato da più utenti, ma l'utente dovrà inserire le informazioni mancanti quando il profilo viene installato. Se personalizzi il profilo per ogni utente, e includi le password, dovresti distribuire il profilo in formato codificato per proteggerne il contenuto. Per ulteriori informazioni, consulta "Installare i profili di configurazione" a pagina 39

Per creare un nuovo profilo di configurazione, fai clic sul pulsante Nuovo nella barra degli strumenti di "Utility Configurazione iPhone". Per aggiungere payload al profilo, devi utilizzare l'elenco payload. Quindi, puoi modificare i payload inserendo e selezionando opzioni disponibili nel pannello modifica.

Per modificare un payload, seleziona l'elemento appropriato nell'elenco payload, fai clic sul pulsante Configura, quindi inserisci le informazioni che vedi sullo schermo come descritto di seguito. I campi obbligatori sono contrassegnati da una freccia di colore rosso.

Per alcune impostazioni, ad esempio Wi-Fi, puoi fare clic sul pulsante Aggiungi (+) per aggiungere configurazioni. Per rimuovere una configurazione, fai clic sul pulsante Elimina (–) nella pannello modifica.

Impostazioni generali

Nelle impostazioni generali indichi nome e identificatore di questo profilo, e decidi se gli utenti possono rimuovere il profilo dopo averlo installato.

Il nome inserito viene visualizzato nell'elenco dei profili e appare sul dispositivo una volta installato il profilo di configurazione. Non è obbligatorio che il nome sia univoco, ma è consigliabile usare un nome descrittivo che permetta di identificare il profilo.

L'identificatore di configurazione deve identificare questo profilo in modo univoco e utilizzare il formato com.*nomesocietà.identificatore*, dove "*identificatore*" descrive il profilo. Ad esempio,com.miasocietà.ufficiocasa.

L'identificatore è importante, poiché durante l'installazione di un profilo, il valore viene confrontato con i profili già presenti sul dispositivo. Se l'identificatore è univoco, le informazioni presenti nel profilo vengono aggiunte al dispositivo. Se l'identificatore corrisponde a un profilo già installato, le informazioni nel profilo sostituiscono quelle presenti sul dispositivo, a eccezione delle impostazioni Exchange. Per poter cambiare un account Exchange, è necessario rimuovere il profilo manualmente in modo che i dati associati con l'account possano essere rimossi.

Per impedire a un utente di cancellare un profilo installato su un dispositivo, scegli un'opzione dal menu a comparsa Sicurezza. L'opzione "Con autorizzazione" consente di specificare una password di autorizzazione necessaria per la rimozione del profilo sul dispositivo. Se selezioni l'opzione Mai, il profilo può essere aggiornato con una nuova versione, ma non può essere rimosso.

Impostazioni dei codici

Se non utilizzi politiche codice di Exchange, questo payload ti permette di impostare le politiche del dispositivo. Al suo interno puoi specificare se è obbligatorio un codice per poter utilizzare il dispositivo, oppure indicare le caratteristiche del codice e la frequenza con cui esso deve essere modificato. Quando viene caricato il profilo di configurazione, l'utente riceve immediatamente la richiesta di inserire un codice che soddisfi le politiche selezionate oppure il profilo non verrà installato.

Se utilizzi politiche dispositivo e politiche codice di Exchange, i due gruppi di politiche vengono uniti applicando così impostazioni più rigide. Per informazioni sul supporto delle politiche Exchange ActiveSync, consulta "Microsoft Exchange ActiveSync" a pagina 7.

Sono disponibili le seguenti politiche:

- *Richiedi codice sul dispositivo:* richiede agli utenti di inserire un codice prima di poter utilizzare il dispositivo. Altrimenti, chiunque abbia il dispositivo potrà accedere a tutte le funzioni e a tutte le informazioni che contiene.
- *Consenti valore semplice:* consente agli utenti di utilizzare caratteri sequenziali o ripetuti nei loro codici. Ad esempio, è possibile utilizzare codici come "3333" o "DEFG".
- *Richiede valore alfanumerico:* richiede che il codice contenga almeno una lettera.
- *Lunghezza minima codice:* specifica il numero minimo di caratteri che devono comporre un codice.
- *Numero minimo di caratteri complessi:* indica il numero minimo di caratteri non alfanumerici (ad esempio $, & e !) che devono essere presenti nel codice.
- *Durata massima codice (in giorni):* richiede agli utenti di modificare il proprio codice alla scadenza dell'intervallo specificato.
- *Blocco automatico (in minuti):* il dispositivo si blocca automaticamente se non viene utilizzato per un numero di minuti pari a questo valore. Per sbloccarlo è necessario inserire il codice.
- *Cronologia codice:* se un nuovo codice corrisponde a un codice precedentemente utilizzato, non verrà accettato. Puoi specificare il numero di codici precedenti che devono essere ricordati e utilizzati per tale confronto.
- *Attesa massima per bloccare il dispositivo:* specifica quando il dispositivo può essere sbloccato nuovamente dopo l'utilizzo, senza dover reinserire il codice.

- *Numero massimo di tentativi falliti:* determina il numero di tentativi falliti di inserimento del codice che possono essere compiuti prima che il dispositivo venga inizializzato. Se non cambi questa impostazione, dopo sei tentativi falliti di inserimento del codice, il dispositivo imposta un ritardo prima che possa essere nuovamente inserito un codice. L'intervallo di tempo aumenta a ogni tentativo non riuscito. Dopo l'undicesimo tentativo fallito, tutti i dati e le impostazioni vengono eliminati dal dispositivo. I tempi di attesa del codice iniziano sempre dopo il sesto tentativo; pertanto, impostando un valore uguale o inferiore a 6, il dispositivo viene inizializzato non appena viene superato il numero di tentativi specificato.

Impostazioni restrizioni

Utilizza questo payload per specificare le funzionalità del dispositivo che l'utente può utilizzare.

- *Consenti contenuto esplicito:* quando questa opzione è disattivata, il contenuto video o musicale esplicto acquistato da iTunes Store viene nascosto. Il contenuto esplicito è contrassegnato come tale dal fornitore del contenuto, per esempio etichette di registrazione, quando viene venduto tramite iTunes Store.
- *Consenti uso di Safari:* quando questa opzione è disattivata, il browser web Safari viene disabilitato e la relativa icona rimossa dalla schermata Home. Inoltre, questo impedisce agli utenti di aprire i clip web.
- *Consenti uso di YouTube:* quando questa opzione è disattivata, l'applicazione YouTube viene disabilitata e la relativa icona rimossa dalla schermata Home.
- *Consenti uso di iTunes Music Store:* quando questa opzione è disattivata, iTunes Music Store viene disabilitato e la relativa icona rimossa dalla schermata Home. Gli utenti non potranno effettuare anteprime, acquisti o download dei contenuti.
- *Consenti installazione applicazioni:* quando questa opzione è disattivata, App Store viene disabilitato e la relativa icona rimossa dalla schermata Home. Inoltre, gli utenti non potranno installare le applicazione sul dispositivo.
- *Consenti uso della fotocamera:* quando questa opzione è disattivata, la fotocamera viene disabilitata e la relativa icona rimossa dalla schermata Home. Gli utenti non potranno scattare fotografie.

Impostazioni Wi-Fi

Questo payload consente di impostare la modalità di connessione del dispositivo a un network wireless. Puoi aggiungere configurazioni network multiple, facendo clic sul pulsante Aggiungi (+) nel pannello modifica.

Queste impostazioni devono essere specificate e devono soddisfare i requisiti del network affinché l'utente possa usarle per avviare una connessione.

- *SSID (Service Set Identifier):* SSID del network wireless cui si desidera connettersi.
- *Network nascosto:* specifica se il network deve trasmettere la propria identità.

- *Tipo sicurezza:* seleziona un metodo di autenticazione da usare per il network. Sono disponibili le seguenti scelte per network di tipo personale e aziendale.
  - *Nessuno:* il network non utilizza alcuna autenticazione.
  - *WEP:* il network utilizza solo l'autenticazione WEP.
  - *WPA/WPA 2:* il network utilizza solo l'autenticazione WPA.
  - *Qualsiasi:* durante la connessione al network, il dispositivo utilizza l'autenticazione WEP o WPA, ma non si connette a network non autenticati.
- *Password:* inserisci la password per il collegamento al network wireless. Se non inserisci alcun elemento, l'utente dovrà inserire una password.

Impostazioni aziendali

In questa sezione puoi specificare le impostazioni per la connessione ai network aziendali. Queste impostazioni appaiono quando scegli un'impostazione Enterprise nel menu a comparsa "Tipo sicurezza".

Nel pannello Protocolli, puoi specificare i metodi EAP da utilizzare per l'autenticazione e configurare le impostazioni PAC (Protected Access Credential) EAP-FAST.

Nel pannello Autenticazione, puoi specificare le impostazioni di accesso quali nome utente e protocolli di autenticazione. Se hai installato un'identità usando la sezione Credenziali, puoi sceglierla dal menu a comparsa "Certificato identità".

Nel pannello Autorizza, puoi specificare quali certificati debbano essere considerati attendibili al fine di convalidare il server di autenticazione della connessione Wi-Fi. L'elenco Certificati attendibili mostra i certificati aggiunti mediante il pannello Credenziali e permette di selezionare quelli da considerare attendibili. Aggiungi i nomi dei server di autenticazione da considerare attendibili nell'elenco Nomi dei certificati ritenuti attendibili dal server. Puoi specificare un server particolare, ad esempio *server.miasocietà.com* oppure un nome parziale come **.miasocietà.com*.

L'opzione "Consenti eccezioni a quanto ritenuto attendibile" consente agli utenti di decidere di considerare attendibile un server quando non può essere stabilita la catena di attendibilità. Per evitare queste richieste e consentire le connessioni solo con i servizi considerati attendibili, disattiva questa opzione e incorpora tutti i certificati necessari in un profilo.

Impostazioni VPN

Questo payload permette di inserire le impostazioni VPN per la connessione al network. Per aggiungere insiemi multipli di connessioni VPN, fai clic sul pulsante Aggiungi (+).

Per informazioni sui protocolli VPN e i metodi di autenticazione supportati, consulta "VPN" a pagina 9. Le opzioni disponibili variano in base al metodo di protocollo e di autenticazione selezionato.

VPN su richiesta

Per le configurazioni IPSec basate su certificazione, puoi attivare "VPN su richiesta" in modo che venga automaticamente stabilita una connessione VPN quando accedi a determinati domini.

Le opzioni "VPN su richiesta" sono le seguenti:

Impostazione	Descrizione
Sempre	Per qualsiasi indirizzo che includa il dominio specificato, verrà stabilita una connessione VPN.
Mai	Per gli indirizzi che corrispondono al dominio specificato non verrà stabilita una connessione VPN, ma se la funzionalità VPN è già attiva, verrà utilizzata.
Connetti se richiesto	Viene stabilita una connessione VPN per gli indirizzi che corrispondono al dominio specificato solo dopo che si è verificato un errore di ricerca DNS.

Puoi specificare nomi domino utilizzando caratteri jolly, per esempio intra*.esempio.com. Le connessioni LDAP non avviano una connessione VPN; se la connessione VPN non è già stata stabilita da un'altra applicazione, per esempio Safari, la ricerca LDAP fallirà.

Proxy VPN

iPhone supporta proxy VPN manuale e la configurazione proxy automatica utilizzando PAC o WPAD. Per specificare un prozy VPN, seleziona un'opzione dal menu a comparsa "Configurazione proxy".

Per le configurazioni proxy automatiche basate su PAC, seleziona Automatico dal menu a comparsa, quindi inserisci l'URL di un documento PAC. Per informazioni sulle funzionalità PACS e sul formato del documento, consulta "Altre risorse" a pagina 55.

Per le configurazioni WPAD (Web Proxy Autodiscovery), seleziona Automatico dal menu a comparsa. Lascia il campo dell'URL server proxy vuoto; iPhone richiederà il documento WPAD usando DHCP e DNS. Per informazioni su WPAD, consulta "Altre risorse" a pagina 55

Impostazioni di posta elettronica

Questo payload consente di configurare gli account e-mail POP o IMAP dell'utente. Questi account saranno aggiunti al dispositivo e, come avviene per gli account di Exchange, gli utenti dovranno inserire manualmente le informazioni non presenti nel profilo al momento della sua installazione, ad esempio la propria password per l'account.

Gli utenti possono modificare alcune delle impostazioni fornite nel profilo, ad esempio il nome dell'account, la password e i server SMTP alternativi. Se ometti parte di queste informazioni nel profilo, gli utenti riceveranno la richiesta di inserirle al primo accesso all'account.

Per aggiungere altri account di posta, fai clic sul pulsante Aggiungi (+).

Impostazioni di Exchange

Questo payload permette di inserire le impostazioni utente per il server Exchange. Puoi creare un profilo per un particolare utente specificando nome utente, nome host e indirizzo e-mail oppure, puoi fornire solamente il nome host; in questo modo, al momento dell'installazione del profilo gli utenti dovranno inserire gli altri valori.

Se nel profilo specifichi nome utente, nome host e impostazioni SSL, l'utente non potrà modificare tali impostazioni sul dispositivo.

È possibile configurare un solo account Exchange per dispositivo. Quando aggiungi account Exchange, gli altri account, compresi gli account IMAP via Exchange, non sono soggetti a questa operazione. Gli account Exchange aggiunti utilizzando un profilo, vengono eliminati quando il profilo viene rimosso e non possono essere eliminati in altro modo.

Di default, Exchange esegue la sincronizzazione di contatti, calendari ed e-mail. L'utente può modificare queste impostazioni sul dispositivo in Impostazioni > Account compresa la quantità di dati giornalieri da sincronizzare.

Se selezioni l'opzione Usa SSL, assicurati di aggiungere i certificati necessari per l'autenticazione della connessione nel pannello Credenziali.

Per fornire un certificato che identifica l'utente sul Server Exchange ActiveSync, fai clic sul pulsante Aggiungi (+), quindi seleziona un certificato identità da Portachiavi di Mac OS X o da "Archivio certificati" di Windows.

Impostazioni LDAP

Questo payload permette di inserire le impostazioni per la connessione a una directory LDAPv3. Puoi specificare basi di ricerca multiple per ogni directory e configurare connessioni directory multiple, facendo clic sul pulsante Aggiungi (+).

Se selezioni l'opzione Usa SSL, assicurati di aggiungere i certificati necessari per l'autenticazione della connessione nel pannello Credenziali.

Impostazioni CalDAV

Questo payload permette di fornire impostazioni account per la connessione a un server calendario compatibile con CalDAV. Questi account saranno aggiunti al dispositivo e, come avviene per gli account di Exchange, gli utenti dovranno inserire manualmente le informazioni non presenti nel profilo al momento della sua installazione, ad esempio la propria password per l'account.

Se selezioni l'opzione Usa SSL, assicurati di aggiungere i certificati necessari per l'autenticazione della connessione nel pannello Credenziali.

Per configurare altri account, fai clic sul pulsante Aggiungi (+).

Impostazioni calendario sottoscritto

Questo payload permette di aggiungere sottoscrizioni calendario di sola lettura all'applicazione Calendario del dispositivo. Per configurare altre sottoscrizioni, fai clic sul pulsante Aggiungi (+).

Consulta il sito web www.apple.com/it/downloads/macosx/calendars/ per un elenco dei calendari pubblici che possono essere sottoscritti.

Se selezioni l'opzione Usa SSL, assicurati di aggiungere i certificati necessari per l'autenticazione della connessione nel pannello Credenziali.

Impostazioni clip web

Questo payload permette di aggiugnere clip web alla schermata Home del dispositivo dell'utente. I clip web forniscono accesso veloce alle pagine web preferite.

Assicurati che l'URL inserito includa il prefisso http:// oppure https://, affinchè il clip web possa funzionare correttamente.

Per aggiungere un'icona personalizzata, seleziona un documento grafico in formato gif, jpeg o png, con una dimensione di 57 x 57 pixel. L'immagine viene automaticamente ridimensionata e ritagliata, se necessario.

Impostazioni delle credenziali

Questo payload consente di aggiungere certificati e identità al dispositivo.
Per informazioni sui formati supportati, consulta "Certificati e identità" a pagina 10.

Quando installi le credenziali, installa anche i certificati intermedi necessari per stabilire la catena a un certificato attendibile presente sul dispositivo. Per visualizzare l'elenco dei certificati root preinstallati, consulta l'articolo Apple Support all'indirizzo http://support.apple.com/kb/HT2185?viewlocale=it_IT.

Aggiungere credenziali su Mac OS X:

1. Fai clic sul pulsante Aggiungi (+).
2. Nella finestra di dialogo che appare, seleziona un documento PKCS1 o PKSC12, quindi fai clic su Apri.

   Se il certificato o l'identità che desideri installare si trova in Portachiavi, utilizza "Accesso Portachiavi" per esportare l'elemento nel formato .p12. Accesso Portachiavi si trova in /Applications/Utilities. Per aiuto, consulta "Aiuto Accesso Portachiavi", disponibile nel menu Aiuto quando Accesso Portachiavi è aperto.

Per aggiungere credenziali multple al profilo di configurazione, fai nuovamente clic sul pulsante Aggiungi (+).

Aggiungere credenziali su Windows:

1. Fai clic sul pulsante Aggiungi (+).
2. Seleziona la credenziale che desideri installare da "Archivio certificati" di Windows.

   Se la credenziale non è disponibile nel tuo archivio certificati personale, devi aggiungerla e la chiave privata deve essere contrassegnata come esportabile; si tratta di uno dei passi disponibili nella procedura di importazione del certificato. Per poter aggiugere certificati root, è necessario un accesso amministratiivo al computer, e il certificato deve essere aggiunto all'archivio personale.

Se stai utilizzando profili di configurazione multipli, assicurati che i certificati non siano duplicati. Non puoi installare copie multiple dello stesso certificato.

Invece di installare i certificati utilizzando un profilo di configurazione, puoi consentire agli utenti di utilizzare Safari per scaricare i certificati da una pagina web direttamente sui dispositivi. In alternativa, puoi inviare i certificati agli utenti a mezzo e-mail. Per ulteriori informazioni, consulta "Installare identità e certificati root" a pagina 54. Inoltre, puoi utilizzare "Impostazioni SCEP", sotto, per specificare il modo in cui il dispositivo ottiene i certificati over-the-air quando il profilo viene installato.

Impostazioni SCEP

Il payload SCEP consente di specificare le impostazioni utilizzabili dal dispositivo per ottenere certificati da un CA con il protocollo SCEP (Simple Certificate Enrollment Protocol).

Impostazione	Descrizione
URL	Si tratta dell'indirizzo del server SCEP.
Nome	Può essere qualsiasi stringa comprensibile dall'Autorità di certificazione (CA); per esempio, può essere utilizzata per distinguere tra le occorrenze.
Oggetto	La rappresentazione di un nome X.500 rappresentata come una matrice di un OID e un valore. Per esempio, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, che si tradurrebbe come segue: [[["C","US"]], [["O","Apple Inc."]], ..., [["1.2.5.3","bar"]]]
Challenge	Una chiave pre-condivisa che il server SCEP può utilizzare per identificare la richiesta o l'utente.
Dimensione chiave	Seleziona una dimensione chiave e utilizzando i riquadri sotto questo campo, l'uso accettabile della chiave.

Per ulteriori informazioni su come iPhone ottiene i certificati in modalità wireless, consulta "Registrazione e configurazione mediante tecnologia over the air" a pagina 21

Impostazioni avanzate

Il payload Avanzato consente di cambiare il nome APN (Access Point Name) del dispositivo e le impostazioni proxy network. Queste impostazioni definiscono il modo in cui il dispositivo si connette al network del gestore. Queste impostazioni dovrebbero essere modificate solo in seguito a una specifica richiesta da parte del personale del network del gestore. Se errate, queste impostazioni impediscono al dispositivo di accedere ai dati attraverso il network cellulare. Per annullare eventuali modifiche involontarie a queste impostazioni, elimina il profilo dal dispositivo. Apple consiglia di definire le impostazioni di APN in un profilo di configurazione separato dalle altre impostazioni aziendali.

iPhone supporta nomi utenti APN con un limite di 20 caratteri e password con un limite di 32 caratteri.

Modificare i profili di configurazione

In "Utility Configurazione iPhone", puoi selezionare un profilo nell'elenco "Profili configurazione", quindi utilizzare l'elenco payload e i pannelli modifica per effettuare le modifiche. Se necessario, puoi anche importare un profilo selezionando Documento > Aggiungi alla libreria e scegliendo quindi un documento .mobileconfig. Se i pannelli impostazioni non sono visibili, scegli Vista > Mostra dettagli.

Il dispositivo può utilizzare il campo Identificatore nel payload Generali per determinare se si tratta di un nuovo profilo o di un aggiornamento di un profilo esistente. Per sostituire un profilo esistente con il profilo aggiornato, non modificare l'identificatore.

Installare profili di fornitura e applicazioni

Puoi utilizzare "Utility Configurazione iPhone" per installare applicazioni e profilo di fornitura sui dispositivi collegati al computer. Per dettagli, consulta il capitolo 5, "Distribuire le applicazioni per iPhone", a pagina 62.

Installare i profili di configurazione

Dopo aver creato un profilo, puoi collegare un dispositivo e installare il profilo utilizzando "Utility Configurazione iPhone".

In alternativa, puoi distribuire il profilo agli utenti via e-mail oppure pubblicarlo su un sito web. Quando utilizzano i dispositivi per aprire un messaggio e-mail o scaricare il profilo dal web, gli utenti ricevono la richiesta di avviare il processo di installazione.

Installare profili di configurazione con Utility Configurazione iPhone

Puoi installare profili di configurazione direttamente su un dispositivo che è stato aggiornato a iPhone OS 3.0 o versione successiva ed è collegato al computer. Inoltre, puoi utilizzare "Utility Configurazione iPhone" per rimuovere profili precedentemente installati.

Per installare un profilo di configurazione:

1. Collega il dispositivo al computer utilizzando un cavo USB.

   Dopo qualche istante, il dispositivo appare nell'elenco Dispositivi in "Utility Configurazione iPhone".

2. Seleziona il dispositivo, quindi fai clic sul pannello "Profilo configurazione".
3. Seleziona un profilo di configurazione dall'elenco, quindi fai clic su Installa.
4. Tocca Installa sul dispositivo per installare il profilo.

   Quando installi direttamente su un dispositivo utilizzando la tecnologia USB, il profilo di configurazione viene automaticamente firmato e criptato prima di essere trasferito sul dispositivo.

Distribuire i profili di configurazione a mezzo e-mail

Puoi distribuire i profili di configurazione utilizzando un messaggio e-mail. Gli utenti installano il profilo ricevendo il messaggio sul loro dispositivo, quindi toccando l'allegato per installarlo.

Per inviare un profilo di configurazione in un messaggio e-maiil:

1. Fai clic sul pulsante Condividi nella barra degli strumenti di "Utility Configurazione iPhone."

   Nella finestra di dialogo che appare, seleziona un'opzione di sicurezza:

   a. *Nessuno:* viene creato un documento solo testo .mobileconfig. Tale documento può essere installato sul dispositivo. Parte del contenuto del documento è offuscato per impedire azioni di spionaggio nel caso in cui il documento venga esaminato.

   b. *Firma profilo di configurazione:* il documento .mobileconfig viene firmato e non potrà essere installato da un dispositivo se viene alterato. Alcuni campi appaiono offuscati per impedire azioni di spionaggio nel caso in cui il documento venga esaminato. Dopo l'installazione, il profilo può essere solo aggiornato da un profilo con lo stesso identificatore e firmato dalla stessa copia di "Utility Configurazione iPhone".

   c. *Firma e codifica il profilo:* firma il profilo affinché non possa essere alterato; codifica l'intero contenuto in modo che non sia possibile esaminare il profilo e che possa essere installato solo su un dispositivo specifico. Se il profilo contiene password, si consiglia di scegliere questa opzione. Verranno creati documenti .mobileconfig separati per ogni dispositivo che selezioni dall'elenco Dispositivi. Se un dispositivo non appare nell'elenco, potrebbe non essere stato precedentemente collegato al computer per ottenere la chiave di codificazione oppure potrebbe non essere stato aggiornato con iPhone OS 3.0 o versione successiva.

2. Fai clic su Condividi; si apre un nuovo messaggio Mail (Mac OS X) o Outlook (Windows) a cui sono allegati i profili come documenti non compressi. Affinché il dispositivo riconosca e installi il profilo, i documenti non devono essere compressi.

Distribuire i profili di configurazione sul web

Puoi distribuire i profili di configurazione utilizzando un sito web. Gli utenti possono installare il profilo scaricandolo con Safari sui dispositivi. Per distrubire facilmente l'URL agli utenti, invialo tramite SMS.

Per esportare un profilo di configurazione:

1. Fai clic sul pulsante Esporta nella barra degli strumenti di "Utility Configurazione iPhone".

   Nella finestra di dialogo che appare, seleziona un'opzione di sicurezza:

   a. *Nessuno:* viene creato un documento solo testo .mobileconfig. Tale documento può essere installato sul dispositivo. Parte del contenuto del documento è offuscato per impedire azioni di spionaggio nel caso in cui il documento venga esaminato; tutttavia, assicurati che quando pubblichi il documento sul sito web sia accessibile solo agli utenti autorizzati.

b *Firma profilo di configurazione:* il documento .mobileconfig viene firmato e non verrà installato da un device se viene alterato. Dopo l'installazione, il profilo può essere solo aggiornato da un profilo con lo stesso identificatore e firmato dalla stessa copia di "Utility Configurazione iPhone". Parte delle informazioni presenti nel profilo è offuscata per impedire azioni di spionaggio nel caso in cui il documento venga esaminato; tutttavia, assicurati che quando pubblichi il documento sul sito web sia accessibile solo agli utenti autorizzati.

c *Firma e codifica il profilo:* firma il profilo in modo che non possa essere alterato e codifica l'intero contenuto in modo che non sia possibile esaminare il profilo e che sia possibile installarlo solo su un dispositivo specifico. Verranno creati documenti .mobileconfig separati per ogni dispositivo che selezioni dall'elenco Dispositivi.

2 Fai clic su Esporta, quindi seleziona una posizione in cui registrare i documenti .mobileconfig.

I documenti sono pronti per essere pubblicati sul sito web. Non comprimere il documento .mobileconfig; in caso contrario, il dispositivo non sarà in grado di riconoscere o installare il profilo. Inoltre, devi configurare il server web in modo che i documenti .mobileconfig siano trasmessi come documenti application/x-apple-aspen-config.

Server Mac OS X

Se il server web utilizza Mac OS X Server v10.5.3 Leopard o versione successiva, significa che è già configurato per la trasmissione dei documenti .mobileconfig nel formato corretto.

Per i server Mac OS X di versioni antecedenti alla v10.5.3, aggiungi il seguente tipo MIME alle impostazioni Tipo MIME mediante Server Admin:

```
application/x-apple-aspen-config mobileconfig
```

Ciò garantisce che tutti i documenti .mobileconfig siano inviati correttamente ai client, indipendentemente da dove sono archiviati sul server.

In alternativa, aggiungi il tipo MIME a httpd.conf o a uno dei suoi documenti di configurazione secondari, a condizione che la configurazione di Apache consenta la sovrascrittura delle directory:

```
AddType application/x-apple-aspen-config mobileconfig
```

Server web IIS

Se utilizzi un server web IIS, aggiungi il tipo MIME alla pagina Proprietà del server utilizzando Manager IIS. L'estensione è `mobileconfig` e il tipo di documento è `application/x-apple-aspen-config`.

In alternativa, puoi aggiungere queste informazioni a specifici siti utilizzando la sezione Intestazioni HTTP del pannello delle proprietà di un sito web.

Installazione utente dei profili di configurazione scaricati

Puoi fornire agli utenti l'URL da cui scaricare i profili sui propri dispositivi, oppure inviare i profili a un account e-mail a cui possano accedere usando il dispositivo prima che venga configurato con informazioni specifiche dell'azienda.

Quando l'utente scarica il profilo dal web oppure apre l'allegato utilizzando Mail, il dispositivo riconosce il profilo e avvia l'installazione quando l'utente tocca Installa.

Durante l'installazione, gli utenti devono inserire le informazioni necessarie, quali la password non specificata nel profilo e altre informazioni necessaria per le impostazioni specificate.

Inoltre, il dispositivo riceve le politiche di Exchange ActiveSync dal server e le aggiorna (se sono state modificate) a ogni connessione successiva. Se le politiche del dispositivo o di Exchange ActiveSync impongono l'impostazione di un codice, per completare l'installazione l'utente dovrà inserire un codice che soddisfi le regole in vigore.

Inoltre, egli dovrà anche inserire la password eventualmente necessaria per poter utilizzare i certificati inclusi nel profilo.

Se l'installazione non viene completata con successo, ad esempio perché il server Exchange risulta irraggiungibile o l'utente ha annullato il processo, le informazioni inserite dall'utente non potranno essere conservate.

Gli utenti possono cambiare la quantità di messaggi giornalieri da sincronizzare sul dispositivo e decidere quali cartelle di posta (oltre alla cartella di posta in entrata) devono essere sincronizzate. Le opzioni di default sono: tre giorni e tutte le cartelle. Questi valori possono essere modificati selezionando Impostazioni > E-mail, contatti, calendari > *nome account Exchange*.

Rimuovere e aggiornare i profili di configurazione

Gli aggiornamenti del profilo di configurazione non vengono inviati agli utenti. Distribuisci i profili aggiornati agli utenti affinchè possano installarli. Quando l'indicatore del profilo corrisponde ed è firmato dalla stessa copia di "Utility Configurazione iPhone", il nuovo profilo sostituisce il profilo presente sul dispositivo.

Le impostazioni specificate da un profilo di configurazione non possono essere modificate sul dispositivo. Per modificare un'impostazione devi installare un profilo aggiornato. Se il profilo era stato firmato, può essere sostituito solo da un profilo firmato dalla stessa copia di "Utility Configurazione iPhone". Affinché il profilo aggiornato venga riconosciuto come sostitutivo, l'identificatore di entrambi i profili deve corrispondere. Per ulteriori informazioni sull'identificatore, consulta "Impostazioni generali" a pagina 30.

Importante: la rimozione di un profilo di configurazione elimina le politiche e tutti i dati degli account Exchange archiviati sul dispositivo, oltre alle impostazioni VPN, ai certificati e alle altre informazioni associate al profilo, compresi i messaggi di posta.

Se il payload "Impostazioni generali" del profilo specifica che il profilo non può essere rimosso dall'utente, il pulsante Rimuovi non sarà disponibile. Se le impostazioni consentono la rimozione tramite una password di autorizzazione, l'utente dovrà inserire la password dopo aver toccato Rimuovi. Per ulteriori informazioni sulle impostazioni della sicurezza del profilo, consulta "Impostazioni generali" a pagina 30.

Configurare manualmente i dispositivi

3

Questo capitolo descrive come configurare manualmente i dispositivi iPhone e iPod touch.

Se non sono disponibili i profili di configurazione automatica, gli utenti possono configurare manualmente i propri dispositivi. Alcune impostazioni, ad esempio le politiche relative ai codici, possono essere impostate solamente mediante un profilo di configurazione.

Impostazioni VPN

Per modificare le impostazioni relative a VPN, seleziona Impostazioni > Generali > Network > VPN.

Durante la configurazione delle impostazioni VPN, il dispositivo chiede di inserire informazioni basate sulle risposte ricevute dal server VPN. Ad esempio, se il server lo richiede, può esserti richiesto un token RSA SecurID.

Per poter configurare una connessione VPN basata su certificati, sul dispositivo devono essere installati i certificati necessari. Per ulteriori informazioni, consulta "Installare identità e certificati root" a pagina 54.

Non è possibile configurare la tecnologia "VPN su richiesta" sul dispositivo; configurala mediante un profilo di configurazione. consultare "VPN su richiesta" a pagina 34.

Impostazioni proxy VPN

Per tutte le configurazioni devi specificare anche un proxy VPN. Per configurare un unico proxy per tutte le connessioni, tocca Manuale e, se necessario, fornisci l'indirizzo, la porta e l'autenticazione. Per fornire un documento di configurazione proxy automatico al dispositivo, tocca Auto e specifica l'URL del documento PACS. Per specificare una configurazione proxy automatica mediante WPAD, tocca Auto; iPhone cercherà le impostazioni WPAD mediante DHCP e DNS. Consulta "Altre risorse", alla fine di questo capitolo per risorse ed esempi PACS.

Impostazioni di IPSec Cisco

Durante la configurazione manuale del dispositivo per una VPN IPSec Cisco, viene visualizzata una schermata simile alla seguente:

La tabella che segue permette di individuare le impostazioni e le informazioni da inserire:

Campo	Descrizione
Descrizione	Titolo descrittivo che identifica il gruppo di impostazioni.
Server	Nome DNS o indirizzo IP del server VPN a cui desideri effettuare la connessione.
Account	Nome utente dell'account di accesso alla VPN usato dall'utente. Non inserire il nome del gruppo in questo campo.
Password	Frase chiave dell'account di accesso alla VPN usato dall'utente. Lasciare vuoto per l'autenticazione RSA SecurID e CryptoCard oppure se si desidera che l'utente immetta manualmente la propria password a ogni tentativo di connessione.
Usa certificato	Disponibile solo se è installata un'identità .p12 o .pfx contenente un certificato fornito per l'accesso remoto *e* la chiave privata di tale certificato. Se è selezionato Usa certificato, i campi Nome gruppo e Chiave condivisa vengono sostituiti da un campo Identità che permette di scegliere da un elenco di identità installate compatibili con la VPN.
Nome gruppo	Nome del gruppo a cui appartiene l'utente come definito sul serve VPN.
Segreto	Chiave condivisa del gruppo. È la stessa per ogni membro del gruppo a cui è assegnato l'utente. *Non* è la password dell'utente e deve essere specificata per iniziare una connessione.

Impostazioni di PPTP

Durante la configurazione manuale del dispositivo per una VPN PPTP, viene visualizzata una schermata simile alla seguente:

La tabella che segue permette di individuare le impostazioni e le informazioni da inserire:

Campo	Descrizione
Descrizione	Titolo descrittivo che identifica il gruppo di impostazioni.
Server	Nome DNS o indirizzo IP del server VPN a cui desideri effettuare la connessione.
Account	Nome utente dell'account di accesso alla VPN usato dall'utente.
RSA SecurID	Se utilizzi un token RSA SecurID, attiva questa opzione per fare in modo che il campo Password risulti nascosto.
Password	Frase chiave dell'account di accesso alla VPN usato dall'utente.
Livello di criptatura	Il valore di default Auto seleziona il massimo livello di codifica-zione disponibile, partendo da 128 bit per passare a 40 bit e infine a Nessuno. Il massimo è solo 128 bit. Nessuno disattiva la crittografia.
Invia tutto il traffico	Di default è impostato su Sì. Invia tutto il traffico del network su un collegamento VPN. Disattiva per consentire l'uso di tunneling di tipo split che inviano attraverso il server solo il traffico destinato ai server all'interno della VPN. Il traffico rimanente viene inviato diret-tamente a Internet.

Impostazioni di L2TP

Durante la configurazione manuale del dispositivo per una VPN L2TP, viene visualizzata una schermata simile alla seguente:

La tabella che segue permette di individuare le impostazioni e le informazioni da inserire:

Campo	Descrizione
Descrizione	Titolo descrittivo che identifica il gruppo di impostazioni.
Server	Nome DNS o indirizzo IP del server VPN a cui desideri effettuare la connessione.
Account	Nome utente dell'account di accesso alla VPN usato dall'utente.
Password	Password dell'account dell'utente per l'accesso alla VPN.
Segreto	Chiave condivisa (chiave pre-condivisa) dell'account L2TP. È la stessa per tutti gli utenti LT2P.
Invia tutto il traffico	Di default è impostato su Sì. Invia tutto il traffico del network su un collegamento VPN. Disattiva per consentire l'uso di tunneling di tipo split che inviano attraverso il server solo il traffico destinato ai server all'interno della VPN. Il traffico rimanente viene inviato direttamente a Internet.

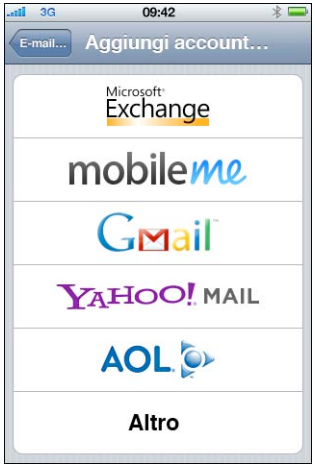
Impostazioni Wi-Fi

Per modificare le impostazioni Wi-Fi, seleziona Impostazioni > Generali > Network > Wi-Fi. Se il network che desideri aggiungere si trova all'interno dell'intervallo, selezionalo dall'elenco dei network disponibili. In caso contrario, tocca Altri.

Verifica che l'infrastruttura del network utilizzi l'autenticazione e la crittografia supportate da iPhone e iPod touch. Per informazioni sulle specifiche, consulta "Protezione di network" a pagina 10. Per informazioni su come installare i certificati per l'autenticazione, consulta"Installare identità e certificati root" a pagina 54.

Impostazioni di Exchange

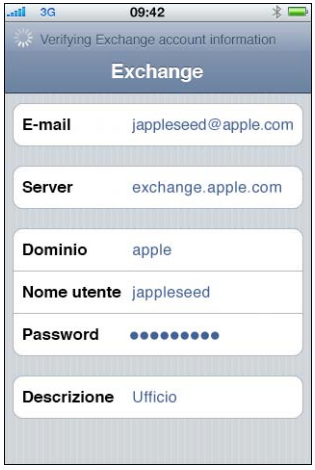
È possibile configurare un solo account Exchange per dispositivo. Per aggiungere un account Exchange, seleziona Impostazioni > E-mail, contatti, calendari e tocca Aggiungi account. Nella schermata Aggiungi account, tocca Microsoft Exchange.



Durante la configurazione manuale del dispositivo per Exchange, utilizza la tabella che segue per identificare le impostazioni e le informazioni da inserire:

Campo	Descrizione
E-mail	Indirizzo e-mail completo dell'utente.
Dominio	Dominio dell'account Exchange dell'utente.
Nome utente	Nome utente dell'account Exchange usato dall'utente.
Password	Password dell'account Exchange dell'utente.
Descrizione	Titolo descrittivo che identifica l'account.

iPhone e iPod touch supportano il servizio Autodiscover di Microsoft, il quale impiega nome utente e password per stabilire l'indirizzo del server Exchange frontale. Se l'indirizzo del server non può essere determinato, il sistema chiede di inserirlo manualmente.



Se il server Exchange cerca una connessione su una porta diversa dalla porta 443, specifica il numero della porta nel campo Server utilizzando il formato *exchange.esempio.com:numeroporta*.

Una volta configurato con successo l'account Exchange, vengono applicate le politiche relative codice del server. Se il codice attuale dell'utente non soddisfa le politiche di Exchange ActiveSync, all'utente viene richiesto di modificarlo o impostare un diverso codice. Il dispositivo potrà comunicare con il server Exchange solo dopo che l'utente avrà impostato un codice appropriato.

Fatto ciò, il dispositivo propone immediatamente di eseguire la sincronizzazione con il server Exchange. Se non desideri eseguire subito la sincronizzazione, potrai avviarla in seguito per calendari e contatti in Impostazioni > E-mail, contatti, calendari. Di default, Exchange ActiveSync invia i nuovi dati al dispositivo non appena questi arrivano sul server. Se preferisci scaricare i nuovi dati mediante una pianificazione o solo in modo manuale, utilizza Impostazioni > E-mail, contatti, calendari > Scarica nuovi dati, per cambiare le impostazioni.

Per modificare la quantità di messaggi e-mail giornalieri da sincronizzare sul dispositivo, seleziona Impostazioni > E-mail, contatti, calendari, quindi seleziona l'account Exchange. Puoi selezionare anche quali cartelle, oltre alla casella di posta in entrata, sono da includere nel recupero delle e-mail push.

Per modificare l'impostazione relativa ai dati di un calendario, seleziona Impostazioni > E-mail, contatti, calendari > Sincronizza.

Impostazioni LDAP

iPhone può cercare le informazioni di contatto sui server directory LDAP. Per aggiungere un server LDAP, seleziona Impostazioni > E-mail, contatti, calendari > Aggiungi account > Altro. Quindi, tocca "Aggiungi account LDAP".

Inserisci l'indirizzo del server LDAP e, se necessario, il nome utente e la password, quindi tocca Successivo. Se il server è raggiungibile e fornisce impostazioni di ricerca di default per il dispositivo, verranno utilizzate tali impostazioni.

Sono supportati le seguenti impostazioni relativamente agli ambiti di ricerca:

Impostazione ambito di ricerca	Descrizione
Base	Cerca solamente nell'oggetto base.
Un livello	Cerca negli oggetti a un livello inferiore dell'oggetto base, ma non nell'oggetto base.
Sottoalbero	Cerca nell'oggetto base e nell'intero albero di tutti gli oggetti che discendono da esso.

Puoi definire diversi insiemi di impostazioni di ricerca per ogni server.

Impostazioni CalDAV

iPhone funziona con i server calendario CalDAV per fornire calendari e programmazioni di gruppo. Per aggiungere un server CalDAV, seleziona Impostazioni > E-mail, contatti, calendari > Aggiungi account > Altro. Quindi, tocca "Aggiungi account CalDAV".

Inserisci l'indirizzo del server CalDAV e, se necessario, il nome utente e la password, quindi tocca Successivo. Dopo aver contattato il server, vengono visualizzati i campi aggiuntivi che ti consentono di impostare altre opzioni.

Impostazioni sottoscrizione calendario

Puoi aggiungere calendari di sola lettura, come programmazioni di progetti o vacanze. Per aggiungere un calendario, seleziona Impostazioni > E-mail, contatti, calendari > Aggiungi account > Altro, quindi tocca "Aggiungi calendario sottoscritto".

Inserisci l'URL di un documento iCalendar (.ics) e, se necessario, il nome utente e la password, quindi tocca Salva. Inoltre, puoi specificare se gli avvisi impostati sul calendario devono essere rimossi quando tale calendario viene aggiunto al dispositivo.

Oltre ad aggiungere manualmente sottoscrizioni calendario, puoi inviare agli utenti un URL webcal:\\ (o un HTTP:\\ ad un documento .ics) e, quando l'utente tocca tale link, il dispositivo chiederà di aggiungerlo come calendario sottoscritto.

Installare identità e certificati root

Se i certificati non vengono distribuiti mediante l'uso di profili, gli utenti possono installarli manualmente utilizzando il dispositivo per scaricarli da un sito web, oppure aprendo un allegato di un messaggio e-mail. Il dispositivo riconosce i certificati con i seguenti tipi MIME ed estensioni di documento:

- application/x-pkcs12, .p12, .pfx
- application/x-x509-ca-cert, .cer, .crt, .der

Per ulteriori informazioni sui formati supportati e sugli altri requisiti, consulta "Certificati e identità" a pagina 10.

Quando scarichi un certificato o un'identità sul dispositivo, viene visualizzata la schermata Installa profilo. La descrizione indica il tipo: identità o autorità di certificazione. Per installare il certificato, tocca Installa. Se si tratta di un certificato identità, dovrai inserire la password del certificato.

Per visualizzare o rimuovere un certificato installato, seleziona Impostazioni > Generali > Profilo. Se rimuovi un certificato necessario per l'accesso a un account o a un network, il dispositivo non potrà più connettersi a tali servizi.

Account e-mail aggiuntivi

Puoi configurare un solo account Exchange, ma se lo desideri, puoi aggiungere altri account POP e IMAP. Per esempio, tali account possono essere utilizzati per accedere alla posta su un server Lotus Notes o Novell Groupwise. Vai su Impostazioni > Account > E-mail, contatti, calendari > Aggiungi account > Altro. Per ulteriori informazioni sull'aggiunta di un account IMAP, consulta il *Manuale utente di iPhone* o il *Manuale utente di iPod touch*.

Aggiornare e rimuovere i profili

Per informazioni su come aggiornare o rimuovere i profili di configurazione, consulta "Rimuovere e aggiornare i profili di configurazione" a pagina 43.

Per informazioni sull'installazione dei profili di fornitura, consulta "Distribuire le applicazioni per iPhone" a pagina 62.

Altre risorse

Per informazioni sul formato e sulla funzione dei documenti di configurazione proxy automatici utilizzati dalle impostazioni proxy VPN, consulta:

- PAC (Proxy auto-config) su http://en.wikipedia.org/wiki/Proxy_auto-config
- Protocollo WPAD (Web Proxy Autodiscovery Protocol) su http://en.wikipedia.org/wiki/Wpad
- Microsoft TechNet "Using Automatic Configuration, Automatic Proxy, and Automatic Detection" disponibile suhttp://technet.microsoft.com/en-us/library/dd361918.aspx

Apple dispone di numerosi tutorial video visualizzabili mediante un browser web standard e che mostrano agli utenti come configurare e utilizzare le funzionalità dei propri iPhone e iPod touch:

- Tour guidato di iPhone, all'indirizzo www.apple.com/it/iphone/guidedtour/
- Tour guidato di iPod touch, all'indirizzo www.apple.com/it/ipodtouch/guidedtour/
- Pagina web di supporto per iPhone, all'indirizzo www.apple.com/it/support/iphone/
- Pagina web di supporto per iPod touch, all'indirizzo www.apple.com/it/support/ipodtouch/

Per ogni dispositivo è disponibile anche un manuale utente in formato PDF che fornisce suggerimenti e dettagli aggiuntivi sull'impiego:

- *Manuale utente di iPhone:* http://manuals.info.apple.com/it_IT/iPhone_Manuale_Utente.pdf
- *Manuale utente di iPod touch:* http://manuals.info.apple.com/it_IT/iPod_touch_3.0_Manuale_utente.pdf

Distribuire iTunes

4

iTunes ti permette di sincronizzare musica e filmati, installare applicazioni e altro ancora.

Questo capitolo descrive come distribuire iTunes e altre applicazioni aziendali, e illustra le impostazioni e le limitazioni che puoi specificare.

Su iPhone e iPod touch puoi sincronizzare qualsiasi tipo di dati (musica, documenti multimediali, ecc.) su un solo computer alla volta. Per esempio, puoi sincronizzare la musica con un computer da scrivania e i preferiti con un un computer portatile, configurando adeguatamente le opzioni di sincronizzazione di iTunes su entrambi i computer. Per ulteriori informazioni sulle opzioni di sincronizzazione, consulta "Aiuto iTunes", disponibile nel menu Aiuto quando iTunes è aperto.

Installazione di iTunes

iTunes utilizza programmi di installazione standard per Macintosh e Windows. Puoi scaricare l'ultima versione di iTunes e un elenco dei requisiti di sistema all'indirizzo www.itunes.com/it.

Per informazioni sui requisiti della concessione in licenza per la distribuzione di iTunes, consulta: http://developer.apple.com/softwarelicensing/agreements/itunes.html

Installazione di iTunes su computer Windows

Quando installi iTunes su computer Windows di default puoi installare la versione più recente di QuickTime, Bonjour e Apple Software Update. Se necessario, puoi omettere questi componenti mediante i parametri del programma di installazione di iTunes, oppure copiando solo i componenti che desideri installare sui computer degli utenti.

Installazione su Windows mediante iTunesSetup.exe

Se desideri utilizzare il normale processo di installazione di iTunes omettendo però alcuni componenti, puoi passare le proprietà a iTunesSetup.exe mediante i parametri della linea di comando.

Proprietà	Significato
NO_AMDS=1	Non installare i servizi Apple Mobile Device Services. Questo componente è necessario affinché iTunes possa eseguire la sincronizzazione e la gestione dei dispositivi mobili.
NO_ASUW=1	Non installare Apple Software Update per Windows. Questa applicazione segnala agli utenti la disponibilità di nuove versioni del software Apple.
NO_BONJOUR=1	Non installare Bonjour. Bonjour garantisce la rilevazione senza configurazione di stampanti, librerie condivise iTunes e altri servizi di network.
NO_QUICKTIME=1	Non installare QuickTime. Questo componente è necessario per l'uso di iTunes. Non omettere QuickTime se non sei certo che sul computer client sia già stata installata l'ultima versione.

Installazione automatica su Windows

Per installare silenziosamente iTunes, estrai i singoli documenti .msi da iTunesSetup.exe, quindi copiali sui computer client.

Per estrarre i documenti .msi da iTunesSetup.exe, esegui le seguenti operazioni:

1. Esegui iTunesSetup.exe.
2. Apri *%temp%* e cerca una cartella chiamata IXP*nnn*.TMP, dove *%temp%* è la tua directory temporanea e *nnn* un numero casuale a 3 cifre. In Windows XP, la directory temporanea di solito si trova in *unità di avvio*:\Documents and Settings*utente*\Impostazioni locali\temp\. In Windows Vista, la directory temporanea di solito si trova in \Utenti*utente*\AppData\Local\Temp\.
3. Copia i documenti .msi dalla cartella a un'altra ubicazione.
4. Esci dal programma di installazione aperto da iTunesSetup.exe.

Fatto ciò, utilizza Preferenze di Editor oggetti Criteri di gruppo della Microsoft Management Console per aggiungere i documenti .msi a una politica Configurazione computer. Assicurati di aggiungere la configurazione a una politica Configurazione computer, invece che a una politica Configurazione utente.

Importante: per funzionare iTunes richiede QuickTime; inoltre, per utilizzare iPod touch o iPhone con iTunes sono necessari i servizi Apple Mobile Device Services (AMDS).

Prima di copiare i documenti .msi, devi selezionare la versione localizzata di iTunes che desideri installare. Per farlo, apri il documento .msi in ORCA, installato Windows SDK come Orca.msi, in bin\. Quindi, modifica lo stream delle informazioni di riepilogo e rimuovi le lingue che non desideri installare. (Locale ID1033 è l'inglese.) In alternativa, utilizza "Editor oggetti Criteri di gruppo" per modificare le proprietà di deployment dei documenti .msi su "Ignora lingua".

Installazione di iTunes su computer Macintosh

I computer Mac sono forniti con iTunes già installato. Puoi scaricare l'ultima versione di iTunes all'indirizzo www.itunes.com/it. Per copiare iTunes sui client Mac, puoi utilizzare Workgroup Manager, uno strumento di amministrazione incluso in Mac OS X Server.

Attivazione rapida dei dispositivi con iTunes

Prima che sia possibile utilizzare iPhone o iPod touch, è necessario attivarli collegandoli ad un computer con iTunes in esecuzione. Normalmente, dopo l'attivazione di un dispositivo, iTunes ti propone di sincronizzare il dispositivo con il computer. Per evitare che questo succeda quando stai configurando un dispositivo per qualcun altro, abilita la modalità di sola attivazione. In questo modo, al termine dell'attivazione, iTunes espelle automaticamente il dispositivo. Il dispositivo è quindi pronto per essere configurato, ma non contiene nessun dato o documento multimediale.

Per abilitare la modalità di sola attivazione in Mac OS X:

1. Assicurati che iTunes non sia in esecuzione, quindi apri Terminale.
2. In Terminale, inserisci un comando:
   - Per abilitare la modalità di sola attivazione:
     ```
     di default: com.apple.iTunes StoreActivationMode -integer 1
     ```
   - Per disabilitare la modalità di sola attivazione:
     ```
     di default: elimina com.apple.iTunes StoreActivationMode
     ```

Per attivare un dispositivo, consulta "Utilizzare la modalità di sola attivazione", a continuazione.

Per abilitare la modalità di sola attivazione in Windows:

1. Assicurati che iTunes non sia in esecuzione, quindi apri una finestra di comandi.
2. Inserisci un comando:
   - Per abilitare la modalità di sola attivazione:
     ```
     "C:\Program Files\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 1
     ```
   - Per disabilitare la modalità di sola attivazione:
     ```
     "C:\Program Files\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 0
     ```

Puoi anche creare un'abbreviazione o modificare quella di iTunes per includere questi comandi, così puoi passare velocemente alla modalità di sola attivazione.

Per verificare che iTunes sia in modalità di sola attivazione, scegli iTunes > Informazioni su iTunes, quindi cerca "solo attivazione" sotto la versione di iTunes e l'identificatore build.

Utilizzare la modalità di sola attivazione

Assicurati di avere abilitato la modalità di sola attivazione così come descritto sopra e segui questi passi.

1. Se attivi iPhone, inserisci una scheda SIM attivata. Utilizza lo strumento di espulsione della SIM oppure una graffetta raddrizzata per espellere il vassoio della SIM. Consulta il *Manuale Utente di iPhone* per maggiori dettagli.
2. Collega iPhone o iPod touch al computer. Perché sia possibile attivare il dispositivo, il computer deve essere connesso a Internet.

   iTunes si apre, se necessario, e attiva il dispositivo. Quando il dispositivo è stato attivato con successo, viene visualizzato un messaggio.
3. Scollega il dispositivo.

   Puoi collegare e attivare immediatamente dispositivi aggiuntivi. Quando la modalità di sola attivazione è abilitata, iTunes non sincronizza alcun dispositivo; quindi non dimenticare di disabilitare tale modalità se pensi di utilizzare iTunes per sincronizzare i dispositivi.

Configurazione delle limitazioni di iTunes

Se necessario, puoi escludere particolari utenti dall'uso di specifiche funzionalità di iTunes. A volte questa operazione viene indicata con il termine Controlli censura.
È possibile limitare l'accesso alle seguenti funzioni:

- Controllo automatico e su comando dell'utente della presenza di nuove versioni di iTunes e di aggiornamenti del software per i dispositivi impiegati
- Visualizzazione dei suggerimenti Genius durante la navigazione o la riproduzione di documenti multimediali
- Sincronizzazione automatica quando i dispositivi sono collegati
- Download della copertina di un album
- Uso dei plugin dei visualizzatori
- Inserimento di un URL di documenti multimediali in streaming
- Ricerca automatica di sistemi Apple TV
- Registrazione di nuovi dispositivi con Apple
- Iscrizione a podcast
- Riproduzione della radio Internet
- Accesso a iTunes Store
- Condivisione della libreria con computer del network locale che eseguono iTunes
- Riproduzione dei contenuti multimediali di iTunes contrassegnati come espliciti
- Riproduzione filmati

- Riproduzione spettacoli TV
- Sincronizzazione dei giochi

Impostazione delle limitazioni di iTunes per Mac OS X

In Mac OS X, puoi controllare l'accesso mediante le chiavi specificate in un documento plist. I valori delle chiavi qui mostrati possono essere specificati per ciascun utente modificando il documento ~/Library/Preferences/com.apple.iTunes.plist con Workgroup Manager, uno strumento di amministrazione fornito con Mac OS X Server.

Per istruzioni su come procedere, consulta l'articolo di Apple Support all'indirizzo http://docs.info.apple.com/article.html?artnum=303099.

Impostazione delle limitazioni di iTunes per Windows

In Windows, puoi controllare l'accesso impostando i valori del registro di sistema all'interno di una delle seguenti chiavi:

Windows XP e Windows Vista a 32 bit:

- HKEY_LOCAL_MACHINE\Software\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Apple Computer, Inc.\iTunes\Parental Controls

Windows Vista a 64 bit:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Wow6432Node\Apple Computer, Inc.\iTunes\Parental Controls

Per informazioni sui valori del registro di sistema di iTunes, consulta l'articolo Apple Support all'indirizzo http://support.apple.com/kb/HT2102?viewlocale=it_IT.

Per informazioni generali sulla modifica del registro di sistema di Windows, consulta la Guida in linea Microsoft e l'articolo del supporto all'indirizzo http://support.microsoft.com/kb/136393.

Aggiornamento manuale del software di iTunes e iPhone

Se disattivi il controllo automatico e avviato dall'utente della disponibilità di aggiornamenti software in iTunes, devi distribuire gli aggiornamenti software agli utenti affinché provvedano all'installazione manuale.

Per aggiornare iTunes, esegui le operazioni di installazione e distribuzione descritte precedentemente in questo documento. Il processo è lo stesso seguito per la distribuzione di iTunes agli utenti.

Per aggiornare il software di iPhone, esegui le seguenti operazioni:

1. Per i computer su cui l'aggiornamento del software di iTunes non è disattivato, usa iTunes per scaricare il software iPhone aggiornato. Per fare ciò, seleziona un dispositivo collegato in iTunes, fai clic sul pannello Riepilogo, quindi sul pulsante "Verifica aggiornamenti".
2. Dopo il download, copia i documenti del programma di aggiornamento (.ipsw) trovati nella seguente posizione:
   - *Su Mac OS X:* ~/Library/iTunes/iPhone Software Updates/
   - *Su Windows XP:* *disco-di-avvio*:\Documents and Settings*nome-utente*\Application Data\Apple Computer\iTunes\iPhone Software Updates\
3. Distribuisci i documenti .ipsw agli utenti, oppure copiali su un'unità del network a cui essi possano accedere.
4. Indica agli utenti di eseguire un backup dei propri dispositivi con iTunes prima di applicare l'aggiornamento. Nota che, durante l'esecuzione di aggiornamenti manuali, iTunes non esegue il backup automatico del dispositivo prima dell'installazione. Per creare un nuovo backup, fai clic col tasto destro (Windows) o fai clic tenendo premuto il tasto Controllo (Mac) sul dispositivo nella barra laterale di iTunes. Fatto ciò, seleziona Backup dal menu contestuale che appare.
5. Per installare gli aggiornamenti, gli utenti possono connettere i propri dispositivi a iTunes e selezionare la linguetta Riepilogo relativa al dispositivo interessato. Fatto ciò, possono procedere tenendo premuto il tasto Opzione (Mac) o Maiusc (Windows) e facendo clic sul pulsante "Verifica aggiornamenti".
6. Viene visualizzata una finestra di dialogo per la selezione dei documenti. Al suo interno, gli utenti possono selezionare i documenti .ipsw e fare clic su Apri per iniziare il processo di aggiornamento.

Creare un backup di iPhone con iTunes

Quando iPhone o iPod touch sono sincronizzati con iTunes, viene eseguito un backup automatico delle impostazioni del dispositivo sul computer. Vengono copiate nella libreria di iTunes anche le applicazioni acquistate su App Store.

Per le applicazioni sviluppate personalmente e distribuite agli utenti con i profili di distribuzione aziendale, non verrà creato alcun backup e le applicazioni non verranno trasferite sul computer dell'utente. Tuttavia, il backup del dispositivo comprenderà qualsiasi documento dati creato dall'applicazione.

I backup del dispositivo possono essere archiviati in formato codificato selezionando l'opzione "Codifica backup iPhone" nel pannello di iTunes con le informazioni di riepilogo del dispositivo. I documenti vengono codificati mediante AES128 con chiave a 256 bit. La chiave viene conservata in modo sicuro nel portachiavi di iPhone.

Nota: se sul dispositivo di cui esegui il backup sono installati profili codificati, iTunes richiede all'utente di abilitare la codificazione dei backup.

Distribuire le applicazioni per iPhone

5

Se desideri, puoi distribuire agli utenti applicazioni per iPhone e iPod touch.

Se desideri installare applicazioni per iPhone OS sviluppate da te, devi distribuirle agli utenti che potranno installarle mediante iTunes.

Le applicazioni scaricate da App Store in linea funzionano su iPhone e iPod touch senza alcuna operazione aggiuntiva. Se hai sviluppato un'applicazione che desideri distribuire personalmente, questa deve essere firmata digitalmente con un certificato emesso da Apple. Inoltre, devi fornire agli utenti un profilo di fornitura di distribuzione che consenta ai loro dispositivi di utilizzare l'applicazione in questione.

Per seguire il processo di distribuzione delle applicazioni devi:

- Registrarti per la distribuzione aziendale con Apple.
- Firmare le applicazioni utilizzando il tuo proprio certificato.
- Creare un profilo di fornitura per la distribuzione aziendale che autorizzi i dispositivi a utilizzare le applicazioni che hai firmato.
- Distribuire l'applicazione e il profilo di fornitura per la distribuzione aziendale sui computer degli utenti.
- Indicare agli utenti di installare l'applicazione e il profilo mediante iTunes.

Per ulteriori informazioni su queste procedure, vedi di seguito.

Registrarsi per lo sviluppo di applicazioni

Per sviluppare e distribuire applicazioni personalizzate per iPhone e iPod touch, devi aderire al programma iPhone Enterprise Developer Program all'indirizzo http://developer.apple.com/.

Una volta completato il processo di registrazione, riceverai istruzioni su come consentire alle tue applicazioni di funzionare sui dispositivi.

Firmare le applicazioni

Le applicazioni distribuite agli utenti devono essere firmate con il tuo certificato di distribuzione. Per informazioni su come ottenere e utilizzare un certificato, consulta l'iPhone Developer Center all'indirizzo http://developer.apple.com/iphone.

Creare il profilo di fornitura per la distribuzione

I profili di fornitura per la distribuzione consentono di creare applicazioni che gli utenti possono utilizzare sui propri iPhone o iPod touch. Per creare un profilo di fornitura per la distribuzione aziendale di una o più specifiche applicazioni, specifica l'AppID autorizzato dal profilo. Se dispone di un'applicazione ma non del profilo che ne autorizza l'impiego, l'utente non sarà in grado di utilizzare tale applicazione.

Il Team Agent aziendale designato può creare i profili di fornitura per la distribuzione dal portale Enterprise Program all'indirizzo http://developer.apple.com/iphone. Per ulteriori informazioni, consulta il sito web.

Una volta creato il profilo di fornitura per la distribuzione aziendale, scarica il documento .mobileprovision e distribuiscilo in modo sicuro assieme alla tua applicazione.

Installare i profili di fornitura mediante iTunes

La copia di iTunes installata dall'utente installa automaticamente i profili di fornitura che si trovano nelle cartelle definite in questa sezione. Se necessario, crea le cartelle utilizzando i nomi mostrati.

Mac OS X

- ~/Library/MobileDevice/Provisioning Profiles/
- /Library/MobileDevice/Provisioning Profiles/
- percorso specificato dalla chiave ProvisioningProfilesPath in ~/Library/Preferences/com.apple.itunes

Windows XP

- *disco-di-avvio*:\Documents and Settings*nome-utente*\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- *disco-di-avvio*:\Documents and Settings\All Users\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- percorso specificato in HKCU o HKLM della chiave di registro SOFTWARE\Apple Computer, Inc\iTunes di ProvisioningProfilesPath

Windows Vista

- *disco-di-avvio*:\Users*nome-utente*\AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- *disco-di-avvio*:\ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- percorso specificato in HKCU o HKLM della chiave di registro SOFTWARE\Apple Computer, Inc\iTunes di ProvisioningProfilesPath

iTunes installa automaticamente i profili di fornitura disponibili nelle posizioni sopra indicate sui dispositivi con cui esegue la sincronizzazione. Una volta installati, i profili di fornitura possono essere visualizzati sul dispositivo in Impostazioni > Generale > Profili.

Inoltre, puoi distribuire il documento .mobileprovision agli utenti e indicare loro di trascinarlo sull'icona dell'applicazione iTunes. In questo modo, iTunes copierà il documento nella posizione corretta specificata in precedenza.

Installare profili di fornitura con Utility Configurazione iPhone

Puoi usare Utility Configurazione iPhone per installare i profili di fornitura sui dispositivi collegati. Per fare ciò, esegui le seguenti operazioni:

1. In "Utility Configurazione iPhone", scegli Archivio > Aggiungi a libreria, quindi seleziona il profilo di fornitura che desideri installare.

   Il profilo viene aggiunto a Utility Configurazione iPhone e può essere visualizzato selezionando la categoria Profili di fornitura nella libreria.
2. Seleziona un dispositivo dall'elenco dei dispositivi collegati.
3. Fai clic sul pannello "Profili di fornitura".
4. Seleziona il profilo di fornitura dall'elenco, quindi fai clic sul pulsante Installa.

Installare applicazioni mediante iTunes

Gli utenti possono utilizzare iTunes per installare le applicazioni sui propri dispositivi. Per consentire questa operazione, distribuisci in modo sicuro l'applicazione agli utenti e indica loro di eseguire le seguenti operazioni:

1. In iTunes, scegli Archivio > Aggiungi alla libreria, quindi seleziona l'applicazione (.app) fornita da te.

   Puoi anche trascinare il documento .app sull'icona dell'applicazione iTunes.
2. Collega un dispositivo al computer, quindi selezionalo nell'elenco Dispositivi in iTunes.
3. Fai clic sul pannello Applicazioni e seleziona l'applicazione dall'elenco.
4. Fai clic su Applica per installare l'applicazione e tutti i profili di fornitura per la distribuzione disponibili nelle cartelle designate, come discusso in "Installare i profili di fornitura mediante iTunes" a pagina 63.

Installare applicazioni con Utility Configurazione iPhone

Puoi usare Utility Configurazione iPhone per installare applicazioni sui dispositivi collegati. Per fare ciò, esegui le seguenti operazioni:

1. In "Utility Configurazione iPhone", scegli Archivio > Aggiungi a libreria, quindi seleziona l'applicazione che desideri installare.

   L'applicazione viene aggiunta a Utility Configurazione iPhone e può essere visualizzata selezionando la categoria Applicazioni nella libreria.
2. Seleziona un dispositivo dall'elenco dei dispositivi collegati.
3. Fai clic sul pannello Applicazioni.
4. Seleziona l'applicazione dall'elenco, quindi fai clic sul pulsante Installa.

Utilizzare le applicazioni aziendali

Quando un utente esegue un'applicazione non firmata da Apple, il dispositivo cerca un profilo di fornitura per la distribuzione che ne autorizzi l'impiego. Se tale profilo non viene trovato, l'applicazione non può essere aperta.

Disabilitare un'applicazione aziendale

Se devi disabilitare un'applicazione interna, puoi farlo revocando l'identità utilizzata per firmare il profilo di fornitura di distribuzione. L'applicazione non potrà più essere installata e, nel caso in cui sia già installata, non si aprirà più.

Altre risorse

Per ulteriori informazioni sulla creazione di applicazioni e profili di fornitura, consulta:

- iPhone Developer Center all'indirizzo http://developer.apple.com/iphone/

Configurazione dei server VPN Cisco

Le linee guida che seguono permettono di configurare il tuo server VPN Cisco per l'uso con iPhone e iPod touch.

Piattaforme Cisco supportate

iPhone supporta i dispositivi di sicurezza adattativi Cisco ASA 5500 e i firewall PIX configurati con il software 7.2.x o versione successiva. È consigliabile utilizzare l'ultima versione rilasciata del software 8.0.x (o versione successiva). iPhone supporta anche i router Cisco IOS VPN con IOS versione 12.4(15)T o versione successiva. I concentratori serie VPN 3000 non supportano le caratteristiche VPN di iPhone.

Metodi di autenticazione

iPhone supporta i seguenti metodi di autenticazione:

- Autenticazione IPSec con chiave pre-condivisa con autenticazione utente mediante xauth.
- Certificati client e server per autenticazione IPsec con autenticazione utente facoltativa mediante xauth.
- Autenticazione ibrida in cui il server fornisce un certificato e il client fornisce una chiave pre-condivisa per l'autenticazione IPsec. È richiesta l'autenticazione utente mediante xauth.
- L'autenticazione utente è effettuata mediante xauth e comprende i seguenti metodi di autenticazione:
  - Nome utente e password
  - SecurID RSA
  - CryptoCard

Gruppi di autenticazione

Il protocollo Cisco Unity impiega i gruppi di autenticazione per riunire gli utenti in base a un insieme comune di parametri di autenticazione e ad altri fattori. Si consiglia di creare un gruppo di autenticazione per gli utenti di iPhone e iPod touch. Per l'autenticazione mediante chiave pre-condivisa e ibrida, il nome del gruppo deve essere configurato sul dispositivo con la relativa chiave pre-condivisa definita come password di gruppo.

La chiave pre-condivisa non è usata in caso di impiego dell'autenticazione mediante certificato se il gruppo dell'utente viene stabilito in base ai campi presenti nel certificato. Le impostazioni del server Cisco possono essere impiegate per mappare i campi di un certificato nei gruppi di utenti.

Certificati

Durante la configurazione e l'installazione dei certificati, verifica quanto segue:

- Il certificato di identità del server deve contenerne il nome DNS e/o l'indirizzo IP nel campo del nome alternativo del soggetto (SubjectAltName). Il dispositivo impiega queste informazioni per verificare che il certificato appartenga al server. Per una maggiore flessibilità, puoi specificare il valore di SubjectAltName utilizzando i caratteri jolly per la corrispondenza dei vari segmenti, ad esempio vpn.*.miasocietà.com. Se non viene specificato il valore di SubjectAltName, è possibile inserire il nome DNS nel campo del nome comune.
- Sul dispositivo dovrebbe essere installato il certificato della CA che ha firmato il certificato del server. Se non si tratta di un certificato root, installa la parte rimanente della catena di trust in modo da garantire l'attendibilità del certificato.
- In caso di utilizzo dei certificati client, verifica che sul server VPN sia installato il certificato della CA attendibile che ha firmato il certificato del client.
- I certificati e le autorità di certificazione devono essere validi (ad esempio, non scaduti).
- L'invio della catena di certificazione da parte del server non è supportato e dovrebbe essere disattivato.
- Durante l'uso dell'autenticazione basata su certificato, verifica che il server sia configurato in modo da identificare il gruppo dell'utente mediante i campi presenti nel certificato del client. Per informazioni, consulta "Gruppi di autenticazione" a pagina 67.

Impostazioni di IPSec

Utilizza le seguenti impostazioni di IPSec:

- *Modalità:* modalità Tunnel.
- *Modalità scambio IKE:* modalità Aggressive per l'autenticazione mediante chiave pre-condivisa e ibrida, modalità Main per l'autenticazione mediante certificato.
- *Algoritmi di codificazione:* 3DES, AES-128, AES-256.
- *Algoritmi di autenticazione:* HMAC-MD5, HMAC-SHA1.
- *Gruppi Diffie Hellman:* per l'autenticazione mediante chiave pre-condivisa e ibrida è necessario il gruppo 2. Per l'autenticazione mediante certificato, utilizza il gruppo 2 con 3DES e AES-128, oppure i gruppi 2 o 5 con AES-256.
- *PFS (Perfect Forward Secrecy):* per IKE fase 2, in caso di utilizzo di PFS il gruppo Diffie Hellman deve essere lo stesso usato per IKE fase 1.
- *Configurazione modalità:* attivata.
- *Rilevamento dead peer:* consigliato.
- *Attraversamento NAT standard:* supportato e attivabile se necessario. IPSec su TCP non supportato.
- *Bilanciamento del carico:* supportato e attivabile se necessario.
- *Re-key della fase 1:* attualmente non supportato. Si consiglia di impostare tempi di re-key sul server di circa un'ora.
- *Maschera indirizzo ASA:* garantisce che tutte le maschere pool del dispositivo siano impostate su 255.255.255.255 oppure non siano impostate. Ad esempio,

  ```
  asa(config-webvpn)# ip local pool vpn_users 10.0.0.1-10.0.0.254 mask
     255.255.255.255.
  ```

  Quando utilizzi la maschera indirizzo consigliata, alcuni percorsi adottati dalla configurazione VPN potrebbero venire ignorati. Per evitarlo, assicurati che la tabella di instradamento contenga tutti i percorsi necessari e controlla che gli indirizzi di sottorete siano accessibili prima del deployment.

Altre funzionalità supportate

iPhone e iPod touch supportano le seguenti funzionalità:

- *Versione delle applicazioni:* la versione del software client viene inviata al server per consentirgli di accettare o respingere le connessioni in base alla versione del software disponibile sul dispositivo.
- *Banner:* se impostato sul server, il banner viene visualizzato sul dispositivo e l'utente può accettarlo o disconnettersi.
- *Split tunneling:* supportato.
- *Split DNS:* supportato.
- *Dominio predefinito:* supportato.

Formato dei profili di configurazione

Questa appendice illustra il formato dei documenti mobileconfig che possono essere impiegati per creare strumenti personalizzati.

Il documento presuppone che il lettore abbia familiarità con il DTD Apple XML e il formato dell'elenco delle proprietà generali. La descrizione generica del formato plist di Apple è disponibile all'indirizzo www.apple.com/DTDs/PropertyList-1.0.dtd.

In questo documento ricorrono spesso i termini *payload* e *profilo*. Si definisce profilo l'intero documento usato per configurare alcune impostazioni (singole o multiple) su dispositivi iPhone o iPod touch. Il payload è un singolo componente del documento profilo.

Livello base

A livello base, il documento di configurazione è un dizionario con le seguenti coppie di chiave/valore:

Chiave	Valore
PayloadVersion	Numero, obbligatorio. Versione del documento profilo di configurazione. Il numero di versione specifica il formato dell'intero profilo, non solo dei singoli payload.
PayloadUUID	Stringa, obbligatorio. Solitamente, una stringa identificatrice univoca generata dal sistema. Il contenuto esatto di questa stringa è irrilevante, tuttavia deve essere univoco a livello globale. In Mac OS X, puoi generare UUID con /usr/bin/uuidgen.
PayloadType	Stringa, obbligatorio. Attualmente l'unico valore valido per questa stringa è "Configuration".
PayloadOrganization	Stringa, facoltativo. Descrive l'organizzazione che emette il profilo come visualizzata all'utente.

Chiave	Valore
PayloadIdentifier	Stringa, obbligatorio. Per convenzione, è una stringa delimitata da punti che descrive il profilo in modo univoco, ad esempio "com.miaSoc.iPhone.impostEmail" o "edu.miaUniv.studenti.vpn". Questa stringa permette di differenziare i profili; se viene installato un profilo che corrisponde all'identificatore di un altro, il primo sovrascrive il secondo (invece di essere aggiunto).
PayloadDisplayName	Stringa, obbligatorio. Specifica una stringa molto breve che può essere visualizzata dall'utente per descrivere il profilo, ad esempio "Impostazioni VPN". Non è obbligatorio che sia univoca.
PayloadDescription	Stringa, facoltativo. Determina il testo descrittivo in formato libero per l'intero profilo da visualizzare all'utente sullo schermo Dettagli. Scopo di questa stringa è di identificare chiaramente il profilo per consentire all'utente di decidere se installarlo.
PayloadContent	Array, facoltativo. È il reale contenuto del profilo. Se omesso, l'intero profilo non ha alcuno scopo pratico.
PayloadRemovalDisallowed	Booleano, facoltativo. Valore di default No. Se impostato, l'utente non potrà eliminare il profilo. È possibile aggiornare un profilo con tale impostazione via USB o via web/e-mail solamente se l'identificatore del profilo corrisponde ed è firmato dalla stessa autorità. Se viene fornita una password di rimozione, il profilo può essere eliminato specificando la password. Con i profili firmati e codificati, l'impostazione di questo valore in chiaro non ha nessuna conseguenza poiché il profilo non può essere alterato e tale impostazione viene mostrata anche sul dispositivo.

Contenuto del payload

L'array PayloadContent è un gruppo di dizionari ognuno dei quali descrive un singolo payload del profilo. Ogni profilo funzionale ha almeno una o più voci in questo array. Ogni dizionario di questo array dispone di alcune proprietà comuni, indipendentemente dal tipo di payload. Altri dizionari sono specializzati e univoci per ciascun tipo di payload.

Chiave	Valore
PayloadVersion	Numero, obbligatorio. Versione del singolo payload. Ogni profilo può essere formato da payload con numeri di versione diversi. Ad esempio, il numero di versione VPN può essere aumentato in futuro mentre il numero di versione di Mail rimane inalterato.
PayloadUUID	Stringa, obbligatorio. Solitamente, una stringa identificatrice univoca generata dal sistema. Il contenuto esatto di questa stringa è irrilevante, tuttavia deve essere univoco a livello globale.
PayloadType	Stringa, obbligatorio. Coppia di chiave/valore che determina il tipo di singolo payload all'interno del profilo.

Chiave	Valore
PayloadOrganization	Stringa, facoltativo. Descrive l'organizzazione che emette il profilo come viene visualizzata dall'utente. Facoltativamente, può essere uguale a PayloadOrganization di livello base.
PayloadIdentifier	Stringa, obbligatorio. Per convenzione, è una stringa delimitata da punti che descrive il payload in modo univoco. Solitamente è il valore PayloadIdentifier base con l'aggiunta di un identificatore secondario; descrive un payload particolare.
PayloadDisplayName	Stringa, obbligatorio. Stringa molto breve visualizzata all'utente per descrivere il profilo, ad esempio "Impostazioni VPN". Non è obbligatorio che sia univoca.
PayloadDescription	Stringa, facoltativo. Determina il testo descrittivo in formato libero per questo payload visualizzato all'utente sullo schermo Dettagli.

Payload password rimozione profilo

Il payload della password di rimozione è designato dal valore com.apple.profileRemovalPassword di PayloadType. Lo scopo è quello di codificare la password che consente agli utenti di rimuovere un profilo di configurazione dal dispositivo. Se il payload è presente e ha un valore impostato per la password, quando l'utente toccherà il pulsante per la rimozione di un profilo il dispositivo richiederà la password. Il payload è codificato con il resto del profilo.

Chiave	Valore
RemovalPassword	Stringa, facoltativo. Specifica la password di rimozione del profilo.

Payload Politica codice

Il payload Politica codice è designato in base al valore di PayloadType di com.apple.mobiledevice.passwordpolicy. La presenza di questo tipo di payload indica a iPhone di visualizzare all'utente un meccanismo di immissione di un codice alfanumerico che permette di immettere codici di lunghezza e complessità arbitrarie.

Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
allowSimple	Booleano, facoltativo. Valore di default YES. Determina se è consentito l'uso di codici semplici. Viene definito semplice un codice contenente caratteri ripetuti o che aumentano/diminuiscono, come ad esempio 123 o CBA. L'impostazione "NO" è sinonimo dell'impostazione del valore "1" per minComplexChars.
forcePIN	Booleano, facoltativo. Valore di default NO. Determina se all'utente deve essere imposto di definire un PIN. L'impostazione semplice di questo valore (ma non di altri) forza l'utente a immettere un codice senza imporne lunghezza o qualità.

Chiave	Valore
maxFailedAttempts	Numero, facoltativo. Di default: 11. Intervallo ammesso [2...11]. Specifica il numero di tentativi consentiti non riusciti di immettere il codice nella schermata di blocco di iPhone. Una volta superato questo valore, il dispositivo viene bloccato e deve essere collegato al programma iTunes per essere sbloccato.
maxInactivity	Numero, facoltativo. Valore di default infinito. Specifica il numero di giorni per cui il dispositivo può rimanere inattivo (senza essere sbloccato dall'utente) prima di venire bloccato dal sistema. Una volta raggiunto il valore specificato, il dispositivo viene bloccato ed è necessario inserire il codice.
maxPINAgeInDays	Numero, facoltativo. Valore di default infinito. Specifica il numero di giorni per cui il codice può rimanere non modificato. Trascorso il numero di giorni specificato, l'utente viene forzato a modificare il codice prima di poter sbloccare il dispositivo.
minComplexChars	Numero, facoltativo. Di default 0. Specifica il numero minimo di caratteri complessi che deve contenere il codice. Viene definito "complesso" ogni carattere diverso da un numero o una lettera, ad esempio &%$#.
minLength	Numero, facoltativo. Di default 0. Specifica la lunghezza complessiva minima del codice. Questo parametro è indipendente dall'altro argomento facoltativo minComplexChars.
requireAlphanumeric	Booleano, facoltativo. Valore di default NO. Specifica se l'utente deve inserire caratteri alfabetici ("abcd") o se sono sufficienti i numeri.
pinHistory	Numero, facoltativo. Quando l'utente modifica il codice, esso deve essere unico rispetto alle ultime N voci contenute nella cronologia. Il valore minimo è 1, quello massimo è 50.
manualFetchingWhenRoaming	Booleano, facoltativo. Se impostato, tutte le operazioni "push" verranno disabilitate quando in roaming. L'utente deve quindi recuperare i nuovi dati manualmente.
maxGracePeriod	Numero, facoltativo. Il periodo di attesa massimo, in minuti, per sbloccare il telefono senza dover inserire un codice. Di default è impostato su 0, quindi viene richiesto immediatamente un codice.

Payload e-mail

Il payload e-mail è designato in base al valore di PayloadType di com.apple.mail.managed PayloadType. Questo payload crea un account e-mail sul dispositivo. Oltre alle impostazioni comuni a tutti i payload, tale payload definisce quanto segue:

Chiave	Valore
EmailAccountDescription	Stringa, facoltativo. Descrizione dell'account e-mail visibile all'utente e mostrata nelle applicazioni Mail e Impostazioni.
EmailAccountName	Stringa, facoltativo. Nome utente completo dell'account. È il nome utente usato nei messaggi inviati, ecc.
EmailAccountType	Stringa, obbligatorio. I valori consentiti sono EmailTypePOP ed EmailTypeIMAP. Definisce il protocollo da utilizzare per l'account.
EmailAddress	Stringa, obbligatorio. Specifica l'indirizzo e-mail completo dell'account. Se assente nel payload, il dispositivo la richiede durante l'installazione del profilo.
IncomingMailServerAuthentication	Stringa, obbligatorio. Indica lo schema di autenticazione per la posta in entrata. I valori consentiti sono EmailAuthPassword ed EmailAuthNone.
IncomingMailServerHostName	Stringa, obbligatorio. Specifica il nome host o l'indirizzo IP del server di posta in entrata.
IncomingMailServerPortNumber	Numero, facoltativo. Indica il numero della porta del server di posta in entrata. Se non viene specificato alcun numero, viene utilizzata la porta di default del protocollo impiegato.
IncomingMailServerUseSSL	Booleano, facoltativo. Valore di default YES. Indica se il server di posta in entrata utilizza SSL per l'autenticazione.
IncomingMailServerUsername	Stringa, obbligatorio. Specifica il nome utente dell'account e-mail; solitamente è la parte di indirizzo e-mail prima del carattere @. Se non presente nel payload quando l'account è configurato in modo da richiedere l'autenticazione per la posta in entrata, il dispositivo richiede questa stringa durante l'installazione del profilo.
IncomingPassword	Stringa, facoltativo. Password per il server di posta in entrata. utilizza solo con profili codificati.
OutgoingPassword	Stringa, facoltativo. Password per il server di posta in uscita. utilizza solo con profili codificati.
OutgoingPasswwordSameAsIncomingPassword	Booleano, facoltativo. Se impostato, la password verrà richiesta solo una volta e verrà utilizzata sia per la posta in uscita che per quella in entrata.
OutgoingMailServerAuthentication	Stringa, obbligatorio. Indica lo schema di autenticazione per la posta in uscita. I valori consentiti sono EmailAuthPassword ed EmailAuthNone.
OutgoingMailServerHostName	Stringa, obbligatorio. Specifica il nome host o l'indirizzo IP del server di posta in uscita.

Chiave	Valore
OutgoingMailServerPortNumber	Numero, facoltativo. Indica il numero della porta del server di posta in uscita. Se non è specificata alcuna porta, vengono usate nell'ordine le porte 25, 587 e 465.
OutgoingMailServerUseSSL	Booleano, facoltativo. Valore di default YES. Indica se il server di posta in uscita utilizza SSL per l'autenticazione.
OutgoingMailServerUsername	Stringa, obbligatorio. Specifica il nome utente dell'account e-mail; solitamente è la parte di indirizzo e-mail prima del carattere @. Se non presente nel payload quando l'account è configurato in modo da richiedere l'autenticazione per la posta in uscita, il dispositivo richiede questa stringa durante l'installazione del profilo.

Payload clip web

Il payload clip web è designato in base al valore PayloadType com.apple.webClip.managed. Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
URL	Stringa, obbligatorio. L'URL che dovrebbe essere aperto dal clip web quando fai clic su di esso. L'URL deve iniziare con HTTP o HTTPS, altrimenti non funzionerà.
Etichetta	Stringa, obbligatorio. Il nome del clip web come visualizzato sulla schermata Home.
Icona	Dati, facoltativo. Un'icona PNG da mostrare nella schermata Home. Le dimensioni dovrebbero essere di 59 x 60 pixel. Se non viene specificato nulla, verrà visualizzata un'icona bianca quadrata.
IsRemovable	Booleano, facoltativo. Se impostato su No, l'utente non può rimuovere il clip web, che però verrà rimosso se viene eliminato il profilo.

Payload LDAP

Il payload LDAP è designato in base al valore PayloadType com.apple.ldap.account. La relazione fra l'account LDAP e LDAPSearchSettings è del tipo one-to-many. Immagina il LDAP come un albero. Ogni oggetto SearchSettings rappresenta un nodo dell'albero in cui iniziare la ricerca e l'ambito in cui effettuare la ricerca (nodo, nodo+1 livello secondario, nodo + tutti i livelli secondari). Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
LDAPAccountDescription	Stringa, facoltativo. Descrizione dell'account.
LDAPAccountHostName	Stringa, obbligatorio. L'host.
LDAPAccountUseSSL	Booleano, obbligatorio. Se utilizzare o meno il protocollo SSL.
LDAPAccountUserName	Stringa, facoltativo. Il nome utente.

Chiave	Valore
LDAPAccountPassword	Stringa, facoltativo. utilizza solo con profili codificati.
LDAPSearchSettings	Oggetto contenitore di livello superiore. Puoi averne molti per un account. Dovresti averne almeno uno per l'account perché sia utile.
LDAPSearchSettingDescription	Stringa, facoltativo. Descrizione di questa impostazione di ricerca.
LDAPSearchSettingSearchBase	Stringa, obbligatoria. Concettualmente, il percorso fino al nodo per iniziare una ricerca in "ou=people,o=example corp"
LDAPSearchSettingScope	Stringa, obbligatoria. Definisce la ricorsione da utilizzare nella ricerca. Può essere uno dei 3 valori seguenti: LDAPSearchSettingScopeBase: Il nodo a cui si dirige immediatamente SearchBase LDAPSearchSettingScopeOneLevel: Il nodo e il suo nodo secondario immediato. LDAPSearchSettingScopeSubtree: Il nodo e tutti i suoi nodi secondari, a prescindere dalla profondità.

Payload CalDAV

Il payload CalDAV è designato dal valore PayloadType com.apple.caldav.account. Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
CalDAVAccountDescription	Stringa, facoltativo. Descrizione dell'account.
CalDAVHostName	Stringa, obbligatorio. L'indirizzo del server
CalDAVUsername	Stringa, obbligatorio. Il nome per il login dell'utente.
CalDAVPassword	Stringa, facoltativo. La password dell'utente
CalDAVUseSSL	Booleano, obbligatorio. Se utilizzare o meno il protocollo SSL.
CalDAVPort	Numero, facoltativo. La porta su cui connettere al server.
CalDAVPrincipalURL	Stringa, facoltativo. L'URL base che dirige al calendario dell'utente.

Payload sottoscrizione calendario

Il payload CalSub è designato dal valore PayloadType com.apple.subscribedcalendar.account. Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
SubCalAccountDescription	Stringa, facoltativo. Descrizione dell'account.
SubCalAccountHostName	Stringa, obbligatorio. L'indirizzo del server.
SubCalAccountUsername	Stringa, facoltativo. Il nome per il login dell'utente

Chiave	Valore
SubCalAccountPassword	Stringa, facoltativo. La password dell'utente.
SubCalAccountUseSSL	Booleano, obbligatorio. Se utilizzare o meno il protocollo SSL.

Payload SCEP

Il payload SCEP (Simple Certificate Enrollment Protocol) è designato in base al valore PayloadType com.apple.encrypted-profile-service. Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
URL	Stringa, obbligatorio.
Nome	Stringa, facoltativa. Qualsiasi stringa che il server SCEP è in grado di capire. Per esempio, potrebbe trattarsi di un nome dominio come esempio.org. Se un'autorità di certificazione possiede diversi certificati CA, questo campo può essere utilizzato per identificare quello richiesto.
Oggetto	Array, facoltativo. La rappresentazione di un nome X.500 rappresentata come una matrice di OID e valore. Per esempio, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, che si tradurrebbe come segue: [[["C","US"]], [["O","Apple Inc."]], ..., [["1.2.5.3","bar"]]] Gli OID possono essere rappresentati come numeri separati da punti, con abbreviazioni per C, L, ST, O, OU, CN (paese, località, stato, società, unità amministrativa, nome comune).
Verifica	Stringa, facoltativo. Una chiave pre-condivisa.
Dimensione chiave	Numero, facoltativo. La dimensione della chiave in bit, 1024 o 2048.
Tipo chiave	Stringa, facoltativo. Attualmente sempre "RSA".
Utilizzo chiave	Numero, facoltativo. Una maschera di bit che indica l'uso della chiave. 1 è la firma, 4 è la codificazione, 5 è entrambe le cose.

Payload APN

Il payload APN (Access Point Name) è designato in base al valore PayloadType di com.apple.apn.managed. Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
DefaultsData	Dizionario, obbligatorio. Contiene due coppie di chiave/valore.
DefaultsDomainName	Stringa, obbligatorio. L'unico valore permesso è com.apple.managedCarrier.

Chiave	Valore
apns	Array, obbligatorio. Contiene un numero arbitrario di dizionari, ognuno dei quali descrive una configurazione APN, seguito dalle coppie di chiavi/valori riportate di seguito.
apn	Stringa, obbligatorio. Specifica il valore di Access Point Name.
username	Stringa, obbligatorio. Specifica il valore del nome utente per questo APN. Se mancante, il dispositivo lo richiede durante l'installazione del profilo.
password	Dati, facoltativo. Rappresentano la password dell'utente di questo APN. Il valore è codificato per scopi di occultamento. Se mancante nel payload, il dispositivo lo richiede durante l'installazione del profilo.
proxy	Stringa, facoltativo. L'indirizzo IP o l'URL del proxy APN.
proxyPort	Numero, facoltativo. Il numero della porta del proxy APN.

Payload Exchange

Il payload è designato in base al valore di PayloadType di com.apple.eas.account. Questo payload crea un account Microsoft Exchange sul dispositivo. Oltre alle impostazioni comuni a tutti i payload, questo definisce quanto segue:

Chiave	Valore
EmailAddress	Stringa, obbligatorio. Se assente nel payload, il dispositivo la richiede durante l'installazione del profilo. Indica l'indirizzo e-mail completo dell'account.
Host	Stringa, obbligatorio. Specifica il nome host o l'indirizzo IP del server Exchange.
SSL	Booleano, facoltativo. Valore di default YES. Indica se il server Exchange utilizza SSL per l'autenticazione.
username	Stringa, obbligatorio. Specifica il nome utente per questo server Exchange. Se mancante, i dispositivi lo richiedono durante l'installazione.
Password	Stringa, facoltativo. La password dell'account. utilizza solo con profili codificati.
Certificato	Facoltativo. Per gli account che consentono l'autenticazione tramite certificato, a .p12 certificato di identità in formato blob NSData.
CertificatePassword	Facoltativo. La password necessaria per il certificato di identità p12. utilizza solo con profili codificati.

Payload di VPN

l payload VPN è designato in base al valore di PayloadType di com.apple.vpn.managed. Oltre alle impostazioni comuni a tutti i tipi di payload, il payload VPN definisce le seguenti chiavi:

Chiave	Valore
UserDefinedName	Stringa. Descrizione della connessione VPN visualizzata sul dispositivo.
OverridePrimary	Booleano. Specifica se inviare tutto il traffico attraverso l'interfaccia VPN. Se True, tutto il traffico di network viene inviato su VPN.
VPNType	Stringa. Determina le impostazioni disponibili nel payload per questo tipo di connessione VPN. Può assumere i valori"L2TP", "PPTP" o "IPSec" che rappresentano rispettivamente L2TP, PPTP e Cisco IPSec.

Sotto le chiavi "PPP" e "IPSec" sono presenti due possibili dizionari al livello superiore. Le chiavi presenti in questi due dizionari sono descritte di seguito assieme al valore VPNType sotto cui esse vengono usate.

Chiavi del dizionario PPP

Gli elementi che seguono riguardano i payload di VPN del tipo PPP.

Chiave	Valore
AuthName	Stringa. Nome utente dell'account VPN. Usato per L2TP e PPTP.
AuthPassword	Stringa, facoltativo. Visibile solo se TokenCard è False. Usato per L2TP e PPTP.
TokenCard	Booleano. Indica se usare una token card per la connessione, ad esempio una card RSA SecurID. Usato per L2TP.
CommRemoteAddress	Stringa. Indirizzo IP o nome host di un server VPN. Usato per L2TP e PPTP.
AuthEAPPlugins	Array. Presente solo se viene utilizzato RSA SecurID; in questo caso è presente una sola voce, una stringa con valore "EAP-RSA". Usato per L2TP e PPTP.
AuthProtocol	Array. Presente solo se viene utilizzato RSA SecurID; in questo caso è presente una sola voce, una stringa con valore "EAP". Usato per L2TP e PPTP.
CCPMPPE40Enabled	Booleano. Vedi la discussione relativa a CCPEnabled. Usato per PPTP.

Chiave	Valore
CCPMPPE128Enabled	Booleano. Vedi la discussione relativa a CCPEnabled. Usato per PPTP.
CCPEnabled	Booleano. Attiva la crittografia sulla connessione. Se questa chiave e CCPMPPE40Enabled sono True, indica il livello di crittografia automatico; se questa chiave e CCPMPPE128Enabled sono True, indica il livello di crittografia massimo. Se la crittografia non viene utilizzata, nessuna delle chiavi CCP è True. Usato per PPTP.

Chiavi del dizionario IPSec

Gli elementi che seguono riguardano i payload di VPN del tipo IPSec.

Chiave	Valore
RemoteAddress	Stringa. Indirizzo IP o nome host del server VPN. Usato per Cisco IPSec.
AuthenticationMethod	Stringa. Può essere "SharedSecret" o "Certificate". Usato per L2TP e Cisco IPSec.
XAuthName	Stringa. Nome utente per l'account VPN. Usato per Cisco IPSec.
XAuthEnabled	Intero. 1 se XAUTH è ON, 0 se OFF. Usato per Cisco IPSec.
LocalIdentifier	Stringa. Presente solo se AuthenticationMethod = SharedSecret. Nome del gruppo da usare. Se viene impiegata l'autenticazione ibrida, la stringa deve terminare con "[hybrid]". Usato per Cisco IPSec.
LocalIdentifierType	Stringa. Presente solo se AuthenticationMethod = SharedSecret. Il valore è "KeyID". Usato per L2TP e Cisco IPSec.
SharedSecret	Dati. Chiave condivisa dell'account VPN. Presente solo se AuthenticationMethod = SharedSecret. Usato per L2TP e Cisco IPSec.
PayloadCertificateUUID	Stringa. UUID del certificato da utilizzare per le credenziali dell'account. Presente solo se AuthenticationMethod = Certificate. Usato per Cisco IPSec.
PromptForVPNPIN	Booleano. Indica se durante la connessione deve essere richiesto un PIN. Usato per Cisco IPSec.

Payload Wi-Fi

Il payload Wi-Fi è designato in base al valore di PayloadType di com.apple.wifi.managed. Questo descrive la versione 0 del valore PayloadVersion. Oltre alle impostazioni comuni a tutti i tipi di payload, il payload definisce le seguenti chiavi:

Chiave	Valore
SSID_STR	Stringa. SSID del network Wi-Fi da utilizzare. Il nome di questa chiave viene dichiarato come APPLE80211KEY_SSID_STR in <Apple80211/Apple80211API.h>.
HIDDEN_NETWORK	Booleano. Oltre a SSID, per differenziare i network il dispositivo impiega informazioni quali tipo di broadcast e di crittografia. Di default, si presuppone che tutti i network configurati siano di tipo aperto o broadcast. Per specificare un network nascosto, è necessario includere un valore booleano per la chiave "HIDDEN_NETWORK" o APPLE80211KEY_HIDDEN_NETWORK.
EncryptionType	Stringa. I valori possibili per "EncryptionType" sono "WEP", "WPA" o "Any". "WPA" corrisponde a WPA e WPA2 e si applica a entrambi i tipi di crittografia. Verifica che questi valori corrispondano esattamente alle caratteristiche del punto di accesso al network. In caso di dubbi sul tipo di crittografia o se desideri applicarlo a tutti i tipi di crittografia, utilizza il valore "Any".
Password	Stringa, facoltativo. L'assenza di una password non impedisce l'aggiunta del network all'elenco dei network noti. All'utente viene richiesto di fornire la password durante la connessione al network in questione.

Per network aziendali 802.1X, è necessario fornire il dizionario di configurazione client EAP.

Dizionario EAPClientConfiguration

Oltre ai tipi di codificazione standard, è possibile utilizzare la chiave "EAPClientConfiguration" per specificare un profilo aziendale per un network particolare. Questa chiave viene dichiarata come kEAPOLControlEAPClientConfiguration in <EAP8021X/EAPOLControlTypes.h>. Se presente, il suo valore è un dizionario contenente le chiavi che seguono.

Chiave	Valore
username	Stringa, facoltativo. Questa proprietà appare nelle configurazioni importate solo se si conosce il nome utente esatto. Gli utenti possono immettere queste informazioni al momento dell'autenticazione.
AcceptEAPTypes	Array di valori interi. Sono accettati i seguenti tipi EAP: 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST
TLSTrustedCertificates	Array di valori dati, facoltativo. Elenco di certificati attendibili per questa autenticazione. Ogni elemento di dati contiene il modulo .cer del certificato corrispondente. Questa chiave permette di personalizzare l'elenco di certificati previsti per un determinato network ed evita di dover chiedere all'utente di impostare dinamicamente il trust su un certificato. Il trust dinamico (finestra di dialogo certificato) è disattivato se questa proprietà è specificata, tranne qualora sia specificata anche TLSAllowTrustExceptions con il valore True (vedi più avanti).
TLSTrustedServerCommonNames	Array di valori stringa, facoltativo. Elenco di nomi comuni dei certificati server che possono essere accettati. Per specificare il nome, puoi utilizzare i caratteri jolly, per esempio wpa.*.esempio.com. I server con certificati non presenti nell'elenco non saranno considerati attendibili. Usata da sola o insieme a TLSTrustedCertificates, questa proprietà consente di indicare precisamente quali certificati devono essere considerati attendibili per il network specificato, evitando così l'uso di certificati con trust dinamico. Il trust dinamico (finestra di dialogo certificato) è disattivato se questa proprietà è specificata, tranne qualora sia specificata anche TLSAllowTrustExceptions con il valore True (vedi più avanti).

Chiave	Valore
TLSAllowTrustExceptions	Booleano, facoltativo. Abilita/disabilita una decisione di trust dinamico da parte dell'utente. Il trust dinamico è la finestra di dialogo del certificato che appare quando questo non è considerato attendibile. In caso di False, l'autenticazione non riesce se il certificato non è già stato considerato attendibile. Vedi TLSTrustedCertificates e TLSTrustedServerCommonNames più indietro. Il valore di default di questa proprietà è True, tranne se sono forniti TLSTrustedCertificates o TLSTrustedServerCommonNames; in questo caso il valore di default è False.
TTLSInnerAuthentication	Stringa, facoltativo. Autenticazione interna usata dal modulo TTLS. Valore di default "MSCHAPv2". I valori possibili sono "PAP", "CHAP", "MSCHAP" e "MSCHAPv2".
OuterIdentity	Stringa, facoltativo. Questa chiave riguarda solamente TTLS, PEAP e EAP-FAST. Consente di nascondere l'identità dell'utente. Il nome reale dell'utente appare solo all'interno del tunnel codificato. Ad esempio, può essere impostato su "anonimo", "anon" o anche "anon@miasocietà.net". Ciò consente di migliorare la protezione, poiché un eventuale malintenzionato non è in grado di vedere il vero nome dell'utente che esegue l'autenticazione.

Supporto di EAP-Fast

Il modulo EAP-FAST impiega le seguenti proprietà nel dizionario EAPClientConfiguration.

Chiave	Valore
EAPFASTUsePAC	Booleano, facoltativo.
EAPFASTProvisionPAC	Booleano, facoltativo.
EAPFASTProvisionPACAnonymously	Booleano, facoltativo.

Queste chiavi sono di natura gerarchica,pertanto se EAPFASTUsePAC è False, le altre due non vengono consultate. Analogamente, se EAPFASTProvisionPAC è False, EAPFASTProvisionPACAnonymously non viene consultata.

Se EAPFASTUsePAC è False, l'autenticazione procede in modo simile a quanto avviene per PEAP o TTLS e il server fornisce la propria identità ogni volta mediante un certificato.

Se EAPFASTUsePAC è Vero, viene utilizzato un PAC esistente (se disponibile). Attualmente, l'unico modo per ottenere un PAC sul dispositivo consiste nell'abilitare la fornitura PAC. A tal fine è necessario abilitare EAPFASTProvisionPAC e, se necessario, EAPFASTProvisionPACAnonymously. Dal punto di vista della protezione EAPFASTProvisionPACAnonymously rappresenta un punto debole poiché non autentica il server, quindi le connessioni sono vulnerabili a un attacco di tipo MITM (man-in-the-middle attack).

Certificati

Come avviene per le configurazioni di VPN, la configurazione dell'identità di un certificato può essere associata a una configurazione Wi-Fi. Ciò è utile durante la definizione delle credenziali per un network aziendale protetto. Per associare un'identità, specificane il payload UUID mediante la chiave "PayloadCertificateUUID".

Chiave	Valore
PayloadCertificateUUID	Stringa. UUID del certificato da utilizzare per le credenziali di identità.

Esempi di profili di configurazione

Questa sezione include esempi di profili utilizzati durante la registrazione e la configurazione over-the-air. Per la descrizione di ogni fase, consulta "Registrazione e configurazione mediante tecnologia over the air" a pagina 21.

Esempio fase 1 risposta del server

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <dict>
        <key>URL</key>
        <string>https://profileserver.example.com/iphone</string>
        <key>DeviceAttributes</key>
        <array>
               <string>UDID</string>
  <string>IMEI</string>
  <string>ICCID</string>
  <string>VERSION</string>
  <string>PRODUCT</string>
        </array>
    <key>Challenge</key>
     <string>optional challenge</string>
     or
     <data>base64-encoded</data>
    </dict>
    <key>PayloadOrganization</key>
    <string>Example Inc.</string>
    <key>PayloadDisplayName</key>
    <string>Profile Service</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
```

```
    <string>fdb376e5-b5bb-4d8c-829e-e90865f990c9</string>
    <key>PayloadIdentifier</key>
    <string>com.example.mobileconfig.profile-service</string>
    <key>PayloadDescription</key>
    <string>Enter device into the Example Inc encrypted profile service</
     string>
    <key>PayloadType</key>
     <string>Profile Service</string>
</dict>
</plist>
```

Esempio fase 2 risposta del dispositivo

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
    <key>Challenge</key>
either:
    <string>String</string>
or:
    <data>"base64 encoded data"</data>
</dict>
</plist>
```

Esempio fase 3 risposta del server con specifiche SCEP

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<dict>
     <key>URL</key>
     <string>https://iphone.vpn.apple.com/pkifoobar.exe</string>
     <key>Name</key>
     <string>instance_for_getcacert_call</string>
     <key>Subject</key>
     <array>
                 <array>
                          <array>
                                   <string>O</string>
                                   <string>Apple Inc.</string>
                          </array>
                 </array>
                 <array>
                          <array>
                                   <string>CN</string>
                                   <string>Foo</string>
                          </array>
                 </array>
     </array>
     <key>Challenge</key>
     <string>CHALLENGE</string>
     <key>Keysize</key>
     <integer>1024</integer>
     <key>Key Type</key>
     <string>RSA</string>
     <key>Key Usage</key>
     <integer>5</integer>
  </dict>
  <key>PayloadDescription</key>
<string>Provides device encryption identity</string>
<key>PayloadUUID</key>
<string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
<key>PayloadType</key>
<string>com.apple.security.scep</string>
<key>PayloadDisplayName</key>
<string>Identità di codificazione</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
```

```
<string>Apple Inc.</string>
<key>PayloadIdentifier</key>
<string>com.apple.encrypted-profile-service</string>
</dict>
</plist>
```

Esempio fase 4 risposta del dispositivo

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
</dict>
</plist>
```